Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Vol. 5 No. 1 (Juli - Oktober 2014)

PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI MENGGUNAKAN *MULTIPLE CRITERIA DECISION ANALYSIS* (MCDA)

INFORMATION SECURITY AWARENESS LEVEL MEASUREMENT USING MULTIPLE CRITERIA DECISION ANALYSIS (MCDA)

Mukhlis Amin
Balai Besar Pengkajian dan Pengembangan Komunikasi dan Informatika (BBPPKI) Makassar
Jl. Prof. Abdurrahman Basalamah II No. 25 Makassar 90234
Emailmukhlis:mukhlis.amin@kominfo..go..idgo.id

diterima: 10 Januari 2014| direvisi: 12 Maret 2014 | disetujui: 15 Mei 2014

Abstract

This study discusses about information security awareness measurement of civil cervant. Assessment of information security awareness determined using Multi Criteria Decision Analysis (MCDA). MCDA method calculate the total value of some alternatives based on value and weight some criteria. The results showed that information security awareness's level of civil servant in Government of Makassar is "avarage". It means action probability required.

Keywords: *Information Security Awareness (ISA), Multiple Criteria Desicion Analysis (MCDA), Governemnt staff*

Abstrak

Penelitian ini membahas mengenai pengukuran tingkat kesadaran keamanan informasi Pegawai Negeri Sipil. Penilaian tingkat kesadaran keamanan informasi dihitung dengan menggunakan metode Multiple Criteria Decision Analysis (MCDA). Metode MCDA menghitung nilai total dari suatu alternatif berdasarkan nilai dan bobot beberapa kriteria yang ada. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi PNS Pemkot Makassar secara keseluruhan berada pada level "sedang" sehingga perlu dimonitor untuk kemungkinan dilakukan pembenahan.

Kata Kunci: Kesadaran Keamanan Informasi, *Multiple Criteria Decision Analysis* (MCDA), staf pemerintahan

Pendahuluan

Era informasi yang semakin berkembang menumbuhkan saling ketergantungan antara manusia satu sama lain di dunia global. Di era ini, setiap orang berpeluang untuk mendapat akses informasi dan pengetahuan baru guna meningkatkan kehidupannya dengan memanfaatkan teknologi-teknologi baru. Namun, hal ini baru dapat terwujud jika saling ketergantungan tersebut diiringi dengan nilai-nilai positif, komitmen dan solidaritas bersama untuk kemajuan pembangunan atas dasar kepentingan bersama. Dalam beberapa tahun terakhir, Asia dan Pasifik telah menjadi 'kawasan superlatif' jika dikaitkan dengan teknologi informasi dan komunikasi (TIK). Menurut International Telecommunication Union, terdapat dua miliar pelanggan telepon dan 1,4 miliar pelanggan telepon seluler di kawasan Asia Pasifik. India dan Cina sendiri mengambil porsi seperempat dari pengguna telepon seluler di dunia pada pertengahan 2008. Kawasan Asia Pasifik juga mewakili 40 persen pengguna Internet dan merupakan pasar broadband terbesar di dunia dengan porsi sebanyak 39 persen dari total dunia. Kehidupan manusia saat ini sangat bergantung pada teknologi informasi dan komunikasi (TIK). Hal ini membuat individu, organisasi dan negara sangat rentan akan serangan terhadap sistem informasi, seperti *hacking, cyberterrorism, cybercrime,* dan lain-lain. Tidak banyak individu dan organisasi yang siap menghadapi serangan-serangan tersebut. Pemerintah memiliki peranan penting untuk memastikan keamanan informasi dengan mengembangkan infrastruktur komunikasi dan informatika dan membangun sistem untuk memberikan perlindungan terhadap ancaman-ancaman keamanan informasi.

Seiring dengan meningkatnya nilai aset informasi, keinginan orang untuk mendapatkan akses informasi dan mengendalikannya juga meningkat. Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi. Pengamanan informasi diperlukan agar kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi tetap terjaga agar tidak mengganggu kinerja dan operasional organisasi. Kegagalan proses pengamanan informasi akan berefek langsung terhadap kepercayaan pelanggan atau masyarakat yang dampaknya dapat mengganggu hingga membawa bencana bagi institusi

bahkan keamanan nasional. Disisi lain perkembangan teknologi telah merubah lingkungan bisnis menjadi lebih terbuka dalam jaringan interkoneksi global (e-World), yang sangat rawan terhadap ancaman. Pertukaran informasi dalam jaringan global telah menjadi target potensial bagi para penyerang baik secara aktif maupun pasif. Hasil survey dari Info Security Europe pada Information Security Breaches Survey 2010 terhadap tipe-tipe pelanggaran keamanan infromasi menunjukkan bahwa penyebab pelanggaran keamanan yang paling banyak adalah pelanggaran yang disebabkan oleh manusia baik secara individu maupun berkelompok (Europe, 2010). Bahkan terdeteksi bahwa pelanggaran paling besar justru dilakukan oleh staf perusahaan atau instansi, baik karena faktor kelalaian hingga faktor kriminal (white collar criminal).

Berdasarkan hal tersebut di atas, manusia memegang peranan kunci dalam penerapan sistem keamanan informasi. Mitnick dan Simon menyatakan manusia merupakan faktor utama dan penting dalam pengamanan informasi selain teknologi, karena manusia merupakan rantai terlemah dalam rantai keamanan (Mitnick & Simon, 2002). Oleh sebab itu, dimensi manusia perlu selalu dibina dengan baik agar segala bentuk ancaman dapat dihindari. Salah satu cara yang dapat dilakukan adalah dengan menumbuhkan kesadaran akan pentingnya keamanan informasi. Kementerian Komunikasi dan Informatika sebagai lembaga negara yang bertanggung jawab dalam pengembangan komunikasi dan informatika memiliki tugas dan tanggung jawab untuk menumbuhkan kesadaran akan pentingnya keamanan informasi kepada masyarakat. Untuk itu, perlu dilakukan penelitian untuk mengukur tingkat kesadaran masyarakat terhadap keamanan informasi guna mengidentifikasi secara mendalam mengenai domain-domain keamanan informasi yang masih perlu ditingkatkan sebagai langkah awal untuk menyusun strategi metode pembinaan keamanan informasi bagi pengguna TI. Penelitian terkait keamanan informasi sudah sangat banyak dilakukan. Namun lebih banyak membahas pada permasalahan teknis. Salah satunya seperti yang telah dilakukan oleh Anjar Priyandoyo. Meskipun dalam penelitian tersebut bertujuan untuk meningkatkan kesadaran keamanan informasi, namun lebih membahas pada kontrol-kontrol teknis keamanan informasi (Priyandoyo, 2006). Berbeda dengan Jumiati dan kawan-kawan yang lebih jauh telah menyusun mekanisme pembinaan kesadaran keamanan informasi di lingkungan Sekolah Tinggi Sandi Negara (Jumiati, Indarjani, & Destrya, 2011). Penelitian lain mengenai kesadaran keamanan informasi yang lebih fokus pada aspek kesadaran manusia (pengguna) pernah dilakukan oleh Michael Wolf dan kawan-kawan. Penelitian tersebut melakukan pengukuran terhadap sebuah program kesadaran keamanan informasi dengan melakukan perbandingan kesadaran pengguna sebelum dan setelah program dilakukan (Wolf, Haworth, & Pietron, 2011), namun hanya fokus pada penggunaan password yang tangguh. Berbeda dengan Kruger dan kawan-kawan yang meneliti apakah "perbedaan budaya dikalangan siswa" memiliki pengaruh pada tingkat kesadaran keamanan sistem informasi mereka (Kruger, Flowerday, Drevin, & Steyn, 2011). Penelitian tersebut dilakukan dengan melakukan tes mengenai pengetahuan, kemampuan menerapkan pengetahuan dan kemampuan untuk memberikan alasan mengenai konsep-konsep keamanan informasi seperi *phising, virus*, *Spam* dan lain-lain. Metode penelitian ini menjadi acuan Hong Chan dalam menyusun tesisnya mengenai tingkat kesadaran keamanan informasi pada karyawan (Chan & Mubarak, 2011). Sebelumnya, Kruger dan Kearney pernah memperkenalkan sebuah prototipe penilaian kesadaran keamanan informasi yang membagi pengukuran menjadi tiga dimensi yaitu pengetahuan, sikap dan perilaku (Krugger & Kearney, 2006). Penelitian tersebut sejalan dengan metode yang digunakan oleh SAI Global dalam mengukur kesadaran keamanan infomasi (Global, 2008). Kruger melakukan pengukuran dengan struktur pohon menggunakan pendekatan *scorecard* sederhana sehingga tingkat kesadaran keamanan informasi dapat diukur baik secara keseluruhan, perdimensi, maupun setiap area fokus keamanan.

Masalah Penelitian

Penelitian ini membahas mengenai tingkat kesadaran keamanan informasi bagi masyarakat yang dikhususkan kepada Pegawai Negeri Sipil sebagai salah satu unsur penting dalam masyarakat. Penilaian tingkat kesadaran keamanan informasi dilakukan dengan mengacu pada prototipe pengukuran kesadaran keamanan informasi yang diperkenalkan oleh Kruger (2011), dengan sedikit melakukan modifikasi dan mempertimbangkan konsep umum keamanan informasi dalam penyusunan instrumen penelitian. Penilaian tingkat kesadaran keamanan informasi dihitung dengan menggunakan metode *Multi Criteria Decision Analysis* (MCDA). Metode MCDA mengitung nilai total dari suatu alternatif berdasarkan nilai dan bobot beberapa kriteria yang ada.

Tinjauan Pustaka

Keamanan Informasi

Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi. Sederhananya, keamanan informasi menghargai nilai informasi dan melindunginya. Terkait keamanan informasi, dikenal istilah 4R keamanan informasi yakni*: Right Information* (Informasi yang benar), *Right People* (Orang yang tepat), *Right Time* (Waktu yang tepat) dan *Right Form* (Bentuk yang tepat). Pengaturan 4R adalah cara paling efisien untuk memelihara dan mengontrol nilai informasi

(APCICT, 2009). *Right Information* mengacu pada ketepatan dan kelengkapan informasi yang menjamin integritas informasi. *Right People* berarti informasi tersedia hanya bagi individu yang berhak yang menjamin kerahasiaan. *Right Time* mengacu pada aksesibilitas informasi dan penggunaannya atas permintaan entitas yang berhak, ini menjamin ketersediaan. Sedangkan *Right Form* mengacu pada penyediaan informasi dalam format yang tepat. Untuk menjaga keamanan informasi, 4R harus digunakan dengan tepat. Ini berarti bahwa kerahasiaan, integritas dan ketersediaan haruslah ditinjau ketika menangani informasi.

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. Phising juga dilakukan dengan caracara non-teknis seperti *Social Engineering* atau dilakukan bersama dengan *Spam* (akan dibahas di bagian berikutnya) sebagai modus untuk melakukan phising. Phising merupakan ancaman umum terhadap aspek kerahasiaan keamanan informasi dan karena itu penting bagi karyawan untuk menyadari konsep dan bahayanya.
2. *Spam*. *Spam* adalah surat atau pesan elektronik komersial yang tidak diinginkan oleh penerimanya. Mungkin tampak sepele, namun *Spam* bukan hanya mengganggu penerima namun berpotensi menimbulkan bencana atau mengganggu sistem. Sebagai contoh, kode berbahaya seperti virus atau trojan sering menggunakan *Spam* sebagai kendaraan untuk distribusi. Kode berbahaya dapat mengurangi performansi sistem dan membatasi akses ke pengguna, sehingga melanggar aspek ketersediaan informasi. Sealin itu dalam pesan *Spam*, terkadang memuat link yang mengarahkan ke situs phising. Sementara kontrol teknis yang diterapkan organisasi untuk mencegah *Spam* memasuki sistem e-mail organisassi mungkin tidak dapat mengatasi 100%. Oleh karena itu, penting baki karyawan atau individu untuk menyadari konsep *Spam* dan bahaya yang terkaut.
3. *Social Engineering*. Dalam konteks keamanan informasi, *Social Engineering* adalah penggunaan sarana non-teknis untuk melakukan pencurian identitas atau untuk memperoleh informasi rahasia. Penyerang dalam hal ini dapat menggunakan kombinasi dari manipulasi psikologis dan peniruan dalam rangka mendorong korban tidak bersedia dalam menyediakan informasi rahasia. Karena aspek yang sangat manusiawi dari *Social Engineering*, tidak mungkin untuk mencegah serangan menggunakan kontrol teknis. Mitigasi *Social Engineering* sangat bergantung pada kesadaran karyawan tentang konsep dan penegakan kebijakan organisasi yang berkaitan dengan keamanan dan privasi.
4. *Strong Password*. Password adalah kunci untuk otentikasi pengguna dan untuk mencegah akses tidak sah kedalam sistem. Selain *Social Engineering* dan praktek phising, password dapat diperoleh secara ilegal dengan menggunakan dua jensi serangan yang dikenal sebagai *password cracking*. Bukan masalahh apakah password dapat dipecahkan atau tidak, melainkan berapa lawa waku yang dibutuhkan untuk memecahkan kombinasi password tersebut. Semakin kuat sebuah password maka semakin lama waktu yang dibutuhkan untuk memecahkannya. Password yang kuat akan mengurangi kemungkinan serangan password dilakukan oleh penyerang. Kontrol teknis yang ada sudah mumpuni untuk membuat password yang kuat, namun tidak semua sistem informasi memiliki kontrol tersebut, oleh karena itu perlu kesadaran karyawan untuk meyakini bahwa password mereka cukup kuat. Pengetahuan mengenai konsep passsword ini menjadi sangat penting. Password yang kuat harus terdiri dari kombinasi yang cukup panjang antara huruf, angka dan simbol.
5. *Data or Information Integrity*. Integritas data dan informasi yang berkaitan dengan aspek integritas keamanan informasi memiliki ciri berikut:
   a. Akurasi dan kebenaran, yaitu informasi harus kuat dan benar dalam artian data harus tepat dan sesuai dengan kenyataan, misalnya data tanggal lahir yang diinputkan ke d alam sistem tidak boleh memiliki ruang kemungkinan kesalahan.
   b. Kepercayaan, memastikan akurasi dan kebenaran akan memastikan bahwa informasi yng tersimpan dalam sistem adalah representasi dari kenyataan sehingga seseorang dapat mempercayai informasi tersebut.
   c. Keberlakuan dan ketepatan waktu, menggunakan tanggal lahir sebagai contoh, tanggal pasti kelahiran adalah variabel yang berubah dari waktu ke waktu. Informasi keberlakuan dipengaruhi oleh perubahan kenyataan dari waktu ke waktu dan harus dipenuhi.
6. *Social Networking*. Pendapat bahwa media sosial atau situs jejaring seperti Facebook dan Twitter sebagai sumber bocornya informasi rahasia sudah semakin relevan beberapa tahun terakhir ini. Media sosial dapat menjadi sumber kebocoran data ketika karyawan mengungkapkan informasi pribadi dan informasi yang berkaitan dengan tempat kerja di situs media sosial. Oleh karena itu, media sosial merupakan bagian penting untuk setiap rencana

keamanan atau kebijakan. Kesadaran akan bahaya jejaring sosial dalam kaitannya dengan keamanan informasi sangatlah penting.

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. Kesadaran keamanan adalah bidang ilmu keamanan yang berhubungan erat dengan faktor manusia mengenai keamanan aset informasi. Pengetahuan yang diperoleh dari sekolah adalah elemen utama untuk menciptakan kesadaran keamanan. Sangat penting untuk mengimplementasikan peraturan keamanan. *Chief Security Officer* bertanggung jawab untuk melakukan program pembelajaran dan atau mengimplementasikan elemen keamanan pada program pembelajaran Teknologi Informasi. 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. Program insentif akan mendorong karyawan untuk berpartisipasi. Kontrol, kewajiban dan hukuman memperlihatkan pentingnya keamanan informasi. Program Kesadaran dan pelatihan keamanan merubah "menjadi sadar" menjadi "menyadari" dan berakhir pada "sadar" yang mengubah budaya keamanan secara total.

Dhillon dalam Kruger (2011), berpendapat bahwa perilaku informal merupakan dasar untuk menggambarkan karakteristik seseorang, organisasi, dan tindakan komunikasi yang mempengaruhi informasi. Selain itu, dikatakan juga bahwa pola pembelajaran, budaya, dan struktur norma yang ada merupakan elemen perilaku informal konstituen. Dengan demikian, dapat disimpulkan bahwa manajemen keamanan informasi hanya dapat dilakukan dengan lengkap jika aspek perilaku individu dan kelompok diketahui. Materi keamanan informasi yang banyak digunakan oleh organisasi saat ini terlalu fokus pada kebijakan keamanan. SAI Global mempunya filosofi bahwa agar keamanan informasi lebih efektif, maka selain mengatasi pengetahuan pengguna, sangatlah penting untuk mengatasi sikap dan perilaku mereka (Global, 2008). Diagram Venn yang ditunjukkan pada Gambar 1 memperlihatkan bahwa posisi keamanan organisasi secara keseluruhan dapat ditingkatkan apabila sikap, pengetahuan dan perilaku pengguna sejalan dengan tujuan dan persyaratan keamanan. Sikap pengguna sangat penting karena selain mereka harus percaya bahwa keamanan sangat penting, pengguna sulit untuk bekerja dengan aman, terlepas dari berapa banyak yang mereka ketahui tetang persyaratan keamanan. Sikap memberikan indikasi yang sangat kuat mengenai arahh tindakan karyawan. Pengetahuan penting karena meskipun pengguna percaya bahwa keamanan itu penting, ia tidak bisa mengubah niat itu menjadi sebuah tindakan tanpa pengetahuan dan pemahaman. Akhirnya, tidak peduli apakah orang percaya atau tahu tentang pentingnya keamanan, itu tidak akan mempengaruhi keamanan kecuali mereka berperilaku dengan cara yang aman.

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). Metode pengukuran yang dilakukan berbasis pada teknik yang dipinjam dari bidang ilmu psikologi yang mengatakan bahwa kecenderungan seseorang untuk melakukan sesuatu yang menguntungkan atau tidak menguntungkan terkait oleh

tiga komponen yaitu : *affect, behavior* and *cognition*. Tiga komponen ini digunakan sebagai dasar dan model yang dikembangkan kedalam tiga dimensi yang ekivalen yaitu: 1) Pengetahuan (*Knowledge*); 2) Sikap (*Attitude)*; dan 3) Perilaku (*Behavior)*. Kruger melakukan pengukuran pada ketiga dimensi ini di enam area yang termasuk memiliki resiko yang kritis yaitu:

a. Selalu taat pada aturan perusahaan
b. Menjaga kerahasiaan password dan *Personal Identity Number* (PIN)
c. Menggunakan e-mail dan internet dengan bijaksana
d. Berhati-hati menggunakan perangkat seluler
e. Melaporkan insiden keamanan informasi,
f. Menyadari konsekuensi setiap tindakan

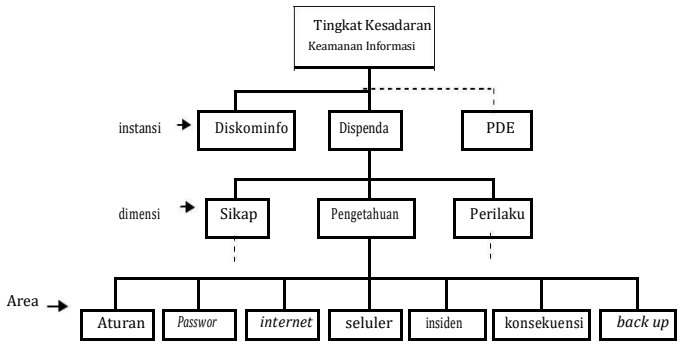
Metode Penelitian

Pengukuran tingkat kesadaran keamanan informasi pegawai negeri sipil di Kota Makassar pada penelitian ini dilakukan di tiga instansi/SKPD yaitu: (1) Dinas Komunikasi dan Informatika; (2) Dinas Pendapatan Daerah dan (3) Kantor Arsip, Perpustakaan dan Pengolahan Data Elektronik. Ketiga instansi ini dipilih karena tupoksi dari instansi-instansi ini sangat berkaitan dengan pemanfaatan teknologi komunikasi dan informatika. Instrumen pengukuran penelitian ini adalah kuesioner yang disebar ke seluruh pegawai negeri sipil di instansi-instansi tersebut. Penentuan responden dilakukan dengan metode judgemental/purposive sampling dimana sampel yang dipilih adalah pegawai negeri sipil di Makassar yang menggunakan internet, komputer dan perangkat seluler. Hal ini dilakukan untuk mengurangi bias hasil penelitian karena antara PNS yang menggunakan dan tidak menggunakan internet, komputer dan perangkat seluler tentunya memiliki pandangan dan pengalaman lain tentang kesadaran keamanan informasi. Selain itu, responden dipilih dari beberapa instansi yang berada pada lokasi yang berbeda dengan harapan dapat mewakili populasi. Pada pelaksanaannya, seluruh pegawai di instansi tersebut diminta untuk mengisi kuesioner, namun hanya pegawai yang memenuhi syarat yang akan dijadikan sampel penelitian. Hal ini dilakukan untuk mempermudah proses pengumpulan data.

Variabel-variabel Pengukuran

Penyusunan instrumen penelitian dilakukan dengan mengacu pada kerangka kerja pengukuran tingkat kesadaran informasi yang telah diperkenalkan oleh Krugger & Kearney (2006) sebagaimana telah dijelaskan pada bagian sebelumnya. Berdasarkan kerangka kerja tersebut dengan sedikit modifikasi yang disesuaikan dengan kondisi penelitian ini maka konsep pengukuran penelitian ini dapat diilustrasikan seperti Gambar 3. Tingkat kesadaran keamanan informasi yang ingin dinilai adalah tingkat kesadaran keamanan informasi secara keseluruhan di Pemerintah kota Makassar. Untuk memperolehnya perlu dilakukan pengukuran kesadaran keamanan informasi di setiap instansi yang dijadikan objek penelitian. Tingkat kesadaran masing-masing instansi diukur berdasarkan tingkat kesadaran keamanan informasi masing-masing dimensi pengetahuan, sikap dan perilaku. Masing-masing dimensi diukur di setiap area keamanan informasi.

Tujuh area kesadaran keamanan informasi ini sesuai dengan enam area pengukuran dalam prototype yang diperkenalkan oleh Krugger & Kearney (2006) ditambahkan dengan satu area yaitu "selalu melakukan Back-up data". Tambahan area ini disesuaikan dengan indeks Keamanan Informasi (KAMI). Indeks KAMI adalah alat evaluasi yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Evaluasi dilakukan terhadap berbagai target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 270001:2005 (Direktorat Jenderal Aptika, 2012). Tingkat Kesadaran Keamanan Informasi dimensi Area Diskominfo Dispenda 2 PDE instansi Sikap Pengetahuan Perilaku Aturan Password internet seluler insiden konsekuensi back up



Gambar 1
Struktur Pohon Konsep Pengukuran
Kesadaran Keamanan Informasi PNS di Makassar

Area-area dalam indeks KAMI antara lain: 1) Peran/Tingkat Kepentingan TIK; 2) Tata Kelola; 3) Pengelolaan Resiko; 4) Kerangka Kerja Keamanan Informasi; 5) Pengelolaan Aset; dan 6) Teknologi dan Keamanan Informasi. Dari beberapa area evaluasi indeks KAMI ini, hanya dua area saja yang memiliki kontrol-kontrol terhadap individu (kesadaran keamanan informasi di sisi pengguna) yaitu Kerangka kerja keamanan informasi dan Pengelolaan aset informasi. Penyesuaian area pengukuran kesadaran keamanan informasi dalam prototype yang diperkenalkan Krugger & Kearney(2006) dengan area evaluasi indeks KAMI sehingga dihasilkan tujuh area pengukuran kesadaran keamanan informasi dalam penelitiaan ini ditunjukkan pada Tabel 1.

Area	Krugger & Kearney(2006)	Indeks KAMI
1.	Selalu taat pada aturan perusahaan	Kontrol 4.20
2.	Menjaga kerahasiaan *password* dan *PIN*.	Kontrol 5.11
3.	Menggunakan e-mail dan internet dengan bijaksana	Kontrol 5.8
4.	Berhati-hati menggunakan perangkat seluler	Kontrol 5.10
5.	Melaporkan insiden keamanan informasi	Kontrol 5.19
6.	Menyadari konsekuensi setiap tindakan	Kontrol 4.7
7.	-	Kontrol 5.22 *(Back up data)*

Tabel 1
Tujuh area pengukuran kesadaran keamanan informasi

Kuesioner penelitian disusun berdasarkan konsep yang telah dipaparkan. Pertanyaan-pertanyaan dikelompokkan kedalam tiga dimensi yaitu pengetahuan (apa yang diketahui), sikap (apa yang dipikirkan) dan perilaku (apa yang dilakukan). Masing-masing dimensi kemudian dibagi kedalam tujuh area keamanan informasi yang telah ditentukan. Yang perlu diperhatikan dalam model ini adalah setiap dimensi dapat memiliki bobot yang berbeda demikian juga dengan setiap area (Krugger & Kearney, 2006). Perlu diidentifikasi apakah setiap area ini dirasa penting, sehingga perlu dilakukan pembobotan berdasarkan tingkat kepentingannya.

Metode Pengukuran

Tingkat kesadaran keamanan informasi dihitung berdasarkan penilaian terhadap jawaban responden. Perhitungan dilakukan dengan metode *Multiple Criteria Decision Analysis* (MCDA). MCDA biasanya digunakan untuk mengambil keputusan atas beberapa alternatif yang memiliki banyak kriteria seperti yang dilakukan oleh Warlina, Rusdiyanto, Sumartono, & Sawir,(2011). Pada penelitian ini, model MCDA digunakan untuk mengukur nilai total alternatif berdasarkan kriteria-kriteria tertentu. Pendekatan MCDA dibedakan menjadi tiga kategori yaitu (Belton & Stewart, 2002): 1) *Value measurement models*; 2) Model perangkingan; dan 3) *Goal programming*. Penelitian ini menggunakan model *value measurement* (pengukuran nilai) untuk mengukur tingkat kesadaran keamanan informasi. Pendekatan ini didasarkan pada perhitungan nilai total kriteria untuk masing-masing alternatif. Nilai dari masing-masing alternatif dalam hal penelitian ini adalah dimensi yang merupakan jumlah nilai keseluruhan kriteria (area kesadaran keamanan informasi) atai sebaliknya perhitungan nilai total masing-masing alternatif (area kesadaran keamanan informasi) yang merupakan jumlah nilai keseluruha kriteria (dimensi). Secara matematis, pendekatan model MCDA ditunjukkan pada persamaan berikut(Belton & Stewart, 2002)

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

Dimana V(a) adalah nilai seluruh alternatif a, v_i (a) adalah nilai skor yang mewakili performansi alternatifa, dan w_i adalah bobot yang diberikan untuk menggambarkan tingkat kepentingan kriteria i.

Nilai v_i (a) ditentukan berdasarkan kuesioner. Empat puluh pertanyaan telah di desain dalam kuesioner untuk menguji pengetahuan, sikap dan perilaku responden berkaitan dengan tujuh area kesadaran keamanan informasi. Setiap pertanyaan diberikan jawaban dengan 3 skala: ya/benar, tidak/salah, dan tidak tahu.

Bobot w_i ditentukan dengan menggunakan *Analytic Hierarchy Process* (AHP). AHP adalah teori pengukuran menggunakan perbandingan berpasangan dan bergantung pada penilaian ahli untuk memperoleh skala prioritas(Saaty, 2008). Kelebihan dari AHP adalah kemampuannya jika dihadapkan pada situasi yang kompleks atau tak berkerangka, dimana data, informasi statistik dari masalah yang dihadapi sangat sedikit. Metoda ini diawali dengan menstrukturkan kondisi yang kompleks ke dalam komponen-komponennya secara hierarki. Setiap hierarki terdiri dari beberapa komponen yang kemudian diuraikan lagi ke dalam hierarki yang lebih rendah, sehingga diperoleh hierarki yang paling rendah, dimana komponen-komponennya dapat dikendalikan. Tahap terpenting dari AHP adalah penilaian perbandingan pasangan. Penilaian ini dilakukan dengan membandingkan sejumlah kombinasi dari elemen yang ada pada setiap tingkat hierarki.

Pendekatan AHP memungkinkan kita melakukan *pair comparison* (perbandingan berpasangan) terhadap masing-masing kriteria area kesadaran keamanan informasi. Perbandingan ini merupakan penilaian subjektif terhadap kriteria-kriteria yang diberikan berdasarkan pendapat dan penilaian manajemen/pakar. Hasil dari penilaian ini lebih mudah disajikan dalam bentuk matriks *pairwise comparisons* yaitu matriks perbandingan berpasangan memuat tingkat preferensi beberapa alternatif untuk tiap kriteria. Skala preferensi yang digunakan yaitu skala 1 yang menunjukkan tingkat yang paling rendah (*equal importance*) sampai dengan skala 9 yang menujukkan tingkatan paling tinggi (*extreme importance*). Penentuan bobot dilakukan dengan menghitung *eigen value* dari matriks tersebut.

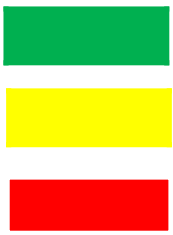
Tabel 2.
Pembobotan Dimensi

Dimensi	Bobot
Pengetahuan	30
Sikap	20

Perilaku	50

Penentuan bobot untuk masing-masing deimensi pengetahuan, sikap dan perilaku ditentukan berdasarkan skala pembobotan yang digunakan oleh Kruger & Kerney(2005). Pembobotan ketiga dimensi tersebut ditunjukkan pada Tabel 2.

Skala tingkat kesadaran keamanan informasi ditentukan ke dalam tiga tingkatan, yaitu: buruk, sedang dan baik. Penentuan skala ditunjukkan pada Gambar 2. Skala ini juga digunakan oleh Kruger & Kerney(2005) dalam mengukur kesadaran keamanan informasi di sebuah perusahaan tambang.



Baik, 80 – 100%

Sedang, 60 – 79%

Buruk, 0 – 59%

Gambar 2.
Skala Tingkat Kesadaran Keamanan Informasi

Hasil Dan Pembahasan

Instrumen penelitian telah disebar kepada seluruh karyawan di tiga instansi pemetintah dan diperoleh sebayak 170 responden. Berdasarkan tujuan dan metode pengumpulan data penelitian, hanya 107 responden yang memenuhi syarat untuk dijadikan sebagai sampel penelitian. Responden yang dinyatakan tidak memenuhi syarat karena responden tersebut menyatakan tidak menggunakan salah satu dari perangkat komputer, internet maupun perangkat seluler. Data responden penelitian ditunjukkan pada Tabel 3.

Tabel 3.
Resonden Penelitian

Instansi	Jumlah kuesioner	Tidak Menggunakan TIK	Jumlah Responden
Dinas Kominfo	52	28	24
Dispenda	58	15	43
Kantor Arsip, Perpustakaan dan PDE	60	20	40
Total	170	63	107

Hasil Pembobotan

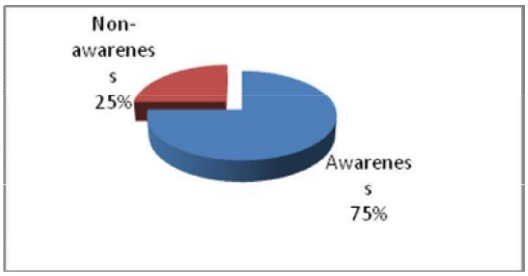
Pembobotan setiap area kesadaran keamanan informasi dilakukan dengan melakukan proses AHP yaitu perhitungan nilai eigen berdasarkan matriks perbandingan. Matriks perbandingan dibuat berdasarkan pertimbangan perbandingan dari pejabat kementerian kominfo yang memiliki tupoksi di bidang keamanan informasi. Hasil perhitungan bobot prioritas dengan menghitung nilai eigen matriks perbandingan ditunjukkan pada Tabel 4. Hasil pembobotan tersebut menunjukkan bahwa bobot area "Selalu taat pada aturan keamanan" memiliki bobot paling tinggi dan sangat jauh berbeda dibandingkan dengan area-area lainnya. Hal ini dapat dikarenakan pemberi pertimbangan lebih menekankan pada penegakan aturan, mengingat pemberi pertimbangan merupakan pejabat kementerian kominfo, dimana tugas kementerian adalah menciptakan regulasi untuk mengatur kehidupan berbangsa dan bernegara. Idealnya, pertimbangan diberikan oleh pihak penanggung jawab keamanan di masing-masing instansi atau setidaknya oleh penanggungjawab keamanan informasi di pemerintahan Kota Makassar. Namun, hal ini sulit dilakukan mengingat pemerintah Kota Makassar belum mengeluarkan suatu regulasi terkait keamanan informasi.

Tabel 4.
Hasil pembobotan Area

Area	w_i
Selalu taat pada aturan	0,564708
Menjaga kerahasiaan *password* dan *PIN.*	0,068242
Menggunakan e-mail dan internet dengan bijaksana	0,039183
Berhati-hati menggunakan perangkat seluler	0,053632
Melaporkan insiden keamanan informasi	0,028627
Menyadari konsekuensi setiap tindakan	0,137525
Selalu melakukan *back-up* data	0,108082

Hasil Pengukuran Kesadaran Keamanan Informasi

Hasil pengukuran tingkat kesadaran keamanan informasi PNS kota Makassar secara keseluruhan diperoleh sebesar 75 % dan berdasarkan skala tingkat kesadaran yang telah ditentukan dalam rancangan penelitian dikategorikan pada tingkat "sedang". Hasil ini menunjukkan bahwa kesadaran keamanan informasi para PNS di Kota Makassar perlu dimonitor terus karena berpotensi memerlukan tindakan pembenahan.



Gambar 3.
Tingkat Kesadaran keseluruhan

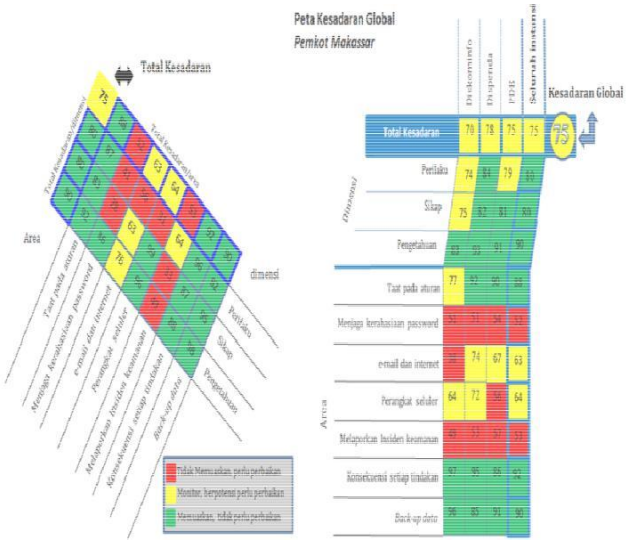
Hasil pengukuran juga disajikan dalam bentuk peta berwarna (lihat Gambar 4) yang menunjukkan secara detail tingkat kesadaran keamanan informasi. Peta ini menunjukkan secara langsung level kesadaran keamanan informasi di setiap instansi yang dilengkapi dengan level kesadaran di setap dimensi dan di setiap area kesadaran keamanan.

Gambar 4 (a) menunjukkan level kesadaran keamanan informasi secara keseluruhan. Kode warna menunjukkan bagian-bagian mana yang tidak memuaskan dan memerlukan perbaikan, bagian-bagian mana yang perlu dimonitor terus yang setiap saat berpotensi untuk dilakukan pembenahan serta bagian-bagian mana yang sudah memuaskan dan perlu dipertahankan. Gambar 4 menunjukkan bahwa kesadaran keamanan informasi secara kesuruhan ditinjau dari masing-masing dimensi sudah baik, namun jika ditinjau dari masing-masing area, terdapat dua area yang meunujukkan tingkat kesadaran keamanan informasi yang tidak memuaskan yaitu area "kerahasiaan *password"* dan "pelaporan insiden keamanan".

Pada area "kerahasiaan *password*" ditunjukkan bahwa yang tidak memuaskan adalah pada dimensi sikap dan perilaku PNS dalam menjaga kerahasiaan *password*-nya, meskipun pada dimensi pengetahuan sudah memuaskan. Berdasarkan tiga bagian program pelatihan dan kesadaran keamanan yang dikemukakan oleh Schlienger & Teufel(2003), penanganan dapat dilakukan dengan melakukan kegiatan-kegiatan yang dapat memotivasi PNS untuk menyadari pentingnya menjaga kerahasiaan *password*, seperti memperbanyak poster, slogan dan produk instansi yang berisi ajakan untuk menjaga kerahasiaan *password* atau informasi mengenai cara-cara menjaga agar *password* tidak mudah diketahui oleh orang lain.

Pada area "pelaporan insiden keamanan" ditunjukkan bahwa dimensi yang kurang memuaskan adalah pada dimensi pengetahuan dan sikap. Jika merujuk pada program pelatihan dan kesadaran keamanan informasi yang dikemukakan oleh Schlienger & Teufel(2003), maka kegiatan yang dapat dilakukan untuk menangani masalah ini adalah dengan memberikan pendidikan dan pelatihan terkait keamanan informasi.

Hasil penelitian juga menunjukkan bahwa ada dua area kesadaran keamanan informasi yang berada pada level sedang yaitu area "penggunaan e-mail dan internet" dan "penggunaan perangkat seluler". Hasil ini merekomendasikan untuk selalu memonitor karena berpotensi untuk dilakukan pembenahan. Jika ditelusuri lebih mendalam, dimensi yang kurang memuaskan pada kedua area ini adalah dimensi perilaku sehingga pembenahan dapat dilakukan dengan selalu memberikan motivasi untuk menjaga keamanan informasi dengan menggunakan e-mail dan internet secara bijaksana dan berhati-hati dalam menggunakan perangkat seluler khususnya di area-area bebas (hotspot/wifi) yang rentan terhadap keamanan informasi.



Gambar 4
(a) Peta Kesadaran Informasi Pemkot Makassar;
(b) Peta Kesadaran Global

Gambar 4 (b) menunjukkan peta kesadaran keamanan informasi secara keseluruhan. Peta global ini menunjukkan bahwa tingkat kesadaran keamanan informasi PNS di masing-masing instansi berada pada tingkat sedang yang artinya perlu dilakukan monitoring. Peta ini juga menunjukkan bahwa semua instansi yang diteliti memiliki tingkat kesadaran keamanan informasi yang kurang memuaskan pada area "kerahasiaan *password*" dan "pelaporan insiden keamanan". Peta juga menunjukkan bahwa instansi yang memiliki tingkat kesadaran keamanan informasi yang kurang memuaskan pada area "penggunaan e-mail dan internet" adalah Dinas Kominfo, sedangkan instansi lainnya masih berada pada level sedang. Instansi yang memiliki tingkat kesadaran keamanan informasi yang kurang memuaskan pada area "penggunaan perangkat seluler" adalah Kantor Arsip, Perpustakaan dan PDE, sedangkan instansi lainnya masih berada pada level sedang. Berdasarkan peta ini, maka area-area yang kurang memuaskan dapat ditentukan secara detail sehingga kegiatan pembenahan bisa lebih spesifik. Informasi yang lebih detail mengenai tingkat kesadaran keamanan

informasi PNS di masing-masing instansi ditunjukkan pada Gambar 6. Keberadaan peta ini, sangat membantu agar program-program kegiatan peningkatan kesadaran keamanan informasi dapat direncanakan dengan lebih matang dan lebih terarah tergantung dengan permasalahan yang dialami masing-masing instansi. Meskipun hasil pengukuran tingkat kesadaran keamanan informasi PNS di kota Makassar pada beberapa area menunjukkan hasil yang tidak memuaskan, namun secara keseluruhan tingkat kesadaran masih menunjukkan hasil yang cukup baik dalam hal ini pada level sedang, dan secara umum level kesadaaran keamanan informasi di setiap dimensi menunjukkan hasil yang memuaskan. Kondisi ini disebabkan bobot kepentingan setiap area yang jauh berbeda. Pada area tertentu yang bernilai memuaskan, juga memiliki bobot tingkat kepentingan yang jauh lebih besar seperti pada area "kepatuhan terhadap aturan keamanan informasi" sehingga meskipun beberapa area bernilai tidak memuaskan, hasil keseluruhan tidak akan signifikan karena bobot kepentingan area yang bernilai buruk tersebut juga jauh lebih kecil dibandingkan area lainnya. Penentuan bobot dengan AHP sudah tepat, namun pertimbangan perbandingan sebaiknya diberikan oleh manajemen internal instansi atau dapat juga dilakukan dengan meminta pertimbangan dari beberapa pakar maupun penanggung jawab keamanan informasi.

Gambar 5.
Peta Tingkat Kesadaran Keamanan Informasi
Masing-masing Instansi Pemkot Makassr:
a) Diskominfo; b) Dispenda; dan c) Kantor Arsip, Perpustakaan dan PDE

Penutup

Kesadaran keaman informasi perlu terus ditingkatkan karena keamanan informasi bukan hanya persoalan teknikal saja, namun konstribusi kelalaian manusia juga berpengaruh dalam kerentanan keamanan informasi. Penelitian ini berusaha mengukur tingkat kesadaran keamanan informasi di kalangan PNS di Kota Makassar dengan harapan dapat memberikan gambaran kondisi kesadaran keamanan informasi di instansi pemerintah khususnya beberapa instansi di Kota Makassar. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi di Pemkot Makassar secara keseluruhan berada pada level "sedang" sehingga perlu dimonitor untuk kemungkinan dilakukan pembenahan. Hasil penelitian juga menunjukkan bahwa tingkat kesadaran setiap dimensi pengetahuan, sikap dan perilaku berada pada level yang memuaskan. Namun demikian, hasil pengukuran juga menunjukkan bahwa ada beberapa area kesadaran keamanan informasi yang tidak memuaskan sehingga perlu dilakukan tindakan seperti:

Menjaga kerahasiaan password. Dimensi sikap (21%) dan Perilaku (41%) perlu mendapat perhatian. Responden mungkin mengetahui pentingnya menjaga kerahasiaan password, namun tidak menyadari bahwa tindakan mereka dapat menyebabkan kebocoran password. Pegawai mungkin merasa bahwa menuliskan password di atas kertas dapat membantu mereka mengingat password mereka, namun hal ini juga dapat menyebabkan orang lain mengetahui password tersebut. Hubungan antar pegawai yang mungkin dekat menyebabkan mereka dengan mudah memberikan password mereka kepada orang lain. Mereka mungkin tidak menyadari bahwa kejaatan keamanan informasi bisa datang dari mana saja.

Pelaporan insiden keamanan. Dimensi pengetahuan (49%) dan sikap (33%) perlu mendapatkan perhatian. Pegawai mungkin belum mengetahui mengenai ciri-ciri serangan keamanan informasi atau merasa tidak peduli jika terjadi serangan dikarenakan ketidaktahuan mereka. Program pelatihan kesadaran keamanan informasi dapat dilakukan untuk menangani masalah ini.

Bijaksana menggunakan e-mail dan internet. Dimensi perilaku (56%) perlu ditingkatkan dengan cara memberikan motivasi melalui selebaran-selebaran atau slogan-slogan berkaitan dengan penggunaan e-mail dan internet secara bijak. Pegawai mungkin tahu, bahwa seenaknya menggunakan e-mail dan internet dapat mengakibatkan serangan keamanan informasi namun tetap melakukannya karena kebutuhan pribadinya. Masalah ini juga dapat diatasi secara teknik, pembatasan hak akses atas situs-situs tertentu perlu dilakukan.

Hasil penelitian ini diharapkan dapat menjadi pertimbangan pemerintah baik pusat dan daerah dalam menangani permasalahan keamanan informasi. Metode pengukuran ini telah menyajikan hasil pengukuran yang sangat lengkap dan detail sehingga penanganan terhadap permasalahan juga dapat dilakukan dengan lebih fokus. Agar model pengukuran ini dapat memberikan hasil yang lebih reliabel, maka perlu dilakukan penelitian lanjutan dengan melakukan beberapa perbaikan antara lain:

a. Menyusun instrumen penelitian berupa pertanyaan-pertanyaan yang lebih banyak dan lebih mendetail agar penilaian terhadap individu lebih akurat. Dapat juga dilakukan dengan menambah skala jawaban kuesioner misalanya dengan skala likert 5 – 7.
b. Mengidentifikasi kembali area-area kesadaran keamanan informasi baik berdasarkan indeks KAMI maupun standar keamanan informasi ISO 27001.
c. Melakukan pembobotan tingkat kepentingan setiap area dengan melibatkan beberapa penanggung jawab atau beberapa pakar keamanan informasi.
d. Meningkatkan konsep pengukuran misalnya dengan membagi pengukuran dalam sub-sub bagian instansi, membagi kedalam beberapa sub area kesadaran keamanan informasi serta melakukan pengukuran pada seluruh instansi bahkan dapat juga diperbesar hingga pengukuran di skala provinsi maupun negara.

Daftar Pustaka

APCICT. (2009). Keamanan Jaringan dan Keamanan Informasi dan Privasi. Dalam APCICT, Akadei Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintah. Incheon: Scandinavian Publishing Co., Ltd.

Belton, V., & Stewart, T. J. (2002). Multiple Criteria Decision Analysis: An Integrated Approach. Kluwer Academic Publishers.

Chan, H., & Mubarak, S. (2011). Information Security Awareness Level of TAFE South Australia Employees.

Direktorat Jenderal Aptika. (2012). Indeks KAMI Versi 2.2. Kementerian Komunikasi dan Informatika.

Europe, I. (2010). Information Security Breaches Survey 2010 (ISBS-2010): Technical Report. PriceWaterHouseCoopers.

Global, S. (2008). Security Awareness: Measuring Attitudes, Knowledge and Behaviour. SAI Global.

Jumiati, Indarjani, S., & Destrya, D. (2011). Pembinaan Kesadaran Keamanan Informasi di Lingkungan Sekolah Tinggi Sandi Negara Berdasarkan Standar National Institute of Standard and Telecommunication (NIST SP 800-100). e-Indonesia Initiative, 394-402.

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An Assessment of the role of cultural factors in information security awareness. ISSA.

Kruger, H., & Kerney, W. (2005). Dipetik Februari 2013, dari icsa.cs.up.ac.za: icsa.cs.up.ac.za/issa/2005/Proceedings/Full/018_Article.pdf

Krugger, H. A., & Kearney, W. D. (2006). A Prototype for assesing information security awareness. Computer & Securitiy, 289 - 296.

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception. Wiley Publishing, Inc.

Papagiannakis, K., Pijl, G. v., & Visser, A. d. (2011). An Overview of the current level of Security Awareness in Greek Companies. Erasmus University of Rottersam.

Priyandoyo, A. (2006). Vulnerability Assesment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi. Jurnal Sistem Informasi.

Saaty, T. L. (2008). Decision Making with the analytic hierarchy process. Int. J. Services Sciences, I(1), 83 - 95.

Schlienger, T., & Teufel, S. (2003). Information Security Culture - From Analysis to Change. South African Computer Journal, 638-646.

Warlina, L., Rusdiyanto, E., Sumartono, & Sawir, I. (2011, September). Dipetik 10 25, 2013, dari http://www.pustaka.ut.ac.id/: http://www.pustaka.ut.ac.id/dev25/pdfprosiding2/fmipa201109.pdf

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring An Information Security Awareness Program. Review of Business Information Systems, 9 – 22.