LAPORAN PELAKSANAAN SURVEY

PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI DI PEMERINTAH KOTA MAKASSAR

KERJA SAMA

Dinas Komunikasi dan Informatika
Kota Makassar
Dan
CV Metadata Institute

2022

DAFTAR ISI

	HALAMAN JUDUL		i
	DAFTAR ISI		ii
	DAFTAR TABEL		iii
	DAFTAR LAMPIRAN		v
BAB I	PENDAHULUAN		1
1.1	Latar Belakang	…….	1
1.2	Maksud dan Tujuan	…….	3
1.3	Landasan Hukum	…….	4
1.4	Hasil Yang Diharapkan	…….	7
BAB II	LANDASAN TEORITIS	…….	5
2.1	Konsep Keamanan Informasi	…….	5
2.2	Kesadaran Keamanan Informasi		8
2.3	Pengukuran Kesadaran Keamanan Informasi		10
2.4	Multi Criteria Decision Making (MCDM)		11
BAB III	Metode Penelitian	…….	17
3.1	Pendekatan Penelitian	…….	17
3,2	Populasi dan Sampel	…….	17
3.3	Jenis Penelitian	…….	18
3.4	Variebel Penelittian	…….	19
3.5	Analisis data	…….	19
BAB IV	Analisis Data	…….	22
4.1	Karkateristik Responden		22
4.2	Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi		25
BAB V	KESIMPULAN DAN REKOMENDASI	…….	35

5.1 Kesimpulan 35
5.2 Rekomendasi 36
DAFTAR PUSTAKA 40
LAMPIRAN 43

DAFTAR TABEL

Tabel 3.1	Hasil Pembobotan Masing-Masing Dimensi	…….	20
Tabel 3.2	Skala Tingkat Kesadaran dan Keamanan Informasi	…….	21
Tabel 4.1	Tingkat Kesadaran Keamanan Informasi Pegawai Pemerintah Kota Makassar	…….	25
Tabel 4.2	Tingkat Kesadaran Keamanan Informasi Berdasarkan Jenis Kelamin	…….	30
Tabel 4.3	Tingkat Kesadaran Keamanan Informasi Antara ASN dan P3K	…….	31
Tabel 4.4	Tingkat Kesadaran Keamanan Informasi Berdasarkan Umur	…….	32
Tabel 4.5	Tingkat Kesadaran Keamanan Informasi Berdasarkan Bidang Pekerjaan	…….	33

Daftar Lampiran

Lampiran 1	Sebaran Responden	 42
Lampiran 2	Kuesioner Survei	 43

BAB I

PENDAHULUAN

1. 1 Latar Belakang

Tak dapat dipungkiri lagi Teknologi Informasi terus berkembang dengan sangat pesat dari waktu ke waktu tanpa mengenal kata berhenti. Perkembangan Teknologi Informasi tersebut tentu saja banyak memberikan dampak positif bagi penggunanya, antara lain mudahnya dalam memperoleh informasi yang dibutuhkan kapanpun dan dimanapun kita berada. Perkembangan Teknologi informasi telah masuk ke seluruh sendi kehidupan manusia salah satunya adalah dalam bidang pendidikan yaitu di kalangan para mahasiswa. Banyak aktivitas mahasiswa yang dilakukan berhubungan dengan teknologi informasi. Baik itu aktivitas umum ataupun yang terkait dengan bidang pendidikan. Banyaknya teknologi informasi yang masuk dalam kehidupan mahasiswa ini tidak akan bermanfaat jika kita hanya sebatas memilikinya saja. Semua teknologi ini akan sangat membantu jika kita dapat memanfaatkan fungsinya secara maksimal dan tepat agar tidak berdampak negatif terhadap diri sendiri dan juga bagi masyarakat sekitar. Namun dibalik itu semua tentu saja selalu ada dampak negatif dari pemanfaatan Teknologi Informasi.

Salah satu dampak negatifnya adalah masalah keamanan (*security*). Ada banyak kasus yang berkaitan dengan keamanan informasi ini. Salah satunya adalah pencurian data ataupun kebocoran informasi masih sangat sering kali terjadi. Contoh sederhana seorang mahasiswa bisa terserang

malware ataupun virus dari penggunaan *flashdisk* tanpa dilakukan *scanning* atau pemindaian menggunakan anti virus, dampaknya bisa jadi data maupun informasi mengenai perkuliahan menjadi hilang atau rusak. Berdasarkan data statistik dalam laporan *Global Cyber Security Index* 2017 yang dirilis *International Telecommunication Union* (ITU) disebutkan dalam rangking tersebut, Indonesia menempati posisi ke-70 dari total 165 negara. Hal ini menunjukkan bahwa betapa buruknya kesadaran masyarakat Indonesia terhadap *security*. Tidak dapat dipungkiri bahwa saat ini akses internet melalui komunikasi nirkabel, baik yang berbayar ataupun fasilitas layanan wifi gratis yang tersedia di bandara, stasiun kereta api dan bangunan komersial meningkat, sehingga memungkinkan terjadinya peningkatan kebocoran informasi. Surat elektronik (email) juga tidak luput menjadi serangan pihak-pihak yang tidak bertanggung jawab. Dimana sebuah email dengan lampiran yang terinfeksi virus dikirim dari penyerang atau adanya kasus laporan *password* yang dicuri atau terinfeksi virus.

Pengamanan informasi perlu dilakukan pada beberapa aspek keamanan informasi diantaranya *Confidentiality, Integrity dan Availability. Confidentiality* adalah keamanan informasi menjamin hak akses suatu informasi kepada pemilik akses informasi. *Integrity* adalah bagaimana menjamin kelengkapan informasi dan menjaga informasi tersebut dari kerusakan atau ancaman dari pihak-pihak yang tidak bertanggung jawab yang berakibat berubah dari aslinya. *Availability* adalah menjamin informasi dapat diakses kapanpun oleh pemilik atau pengguna informasi tanpa terjadi

gangguan atau perubahan informasi tersebut. Perlu kesadaran yang tinggi bagi para pegawai di lingkup Pemerintah Kota Makassar dalam memanfaatkan teknologi informasi tersebut.

1.2 Maksud dan Tujuan

Maksud dan tujuan kegiatan ini adalah:

a. Melakukan pengukuran tingkat kesadaran keamanan informasi ASN dan P3K Pemerintah Kota Makassar
b. Hasil pengukuran tersebut akan menjadi acuan dan strategi dalam Menyusun program kerja Dinas Komunikasi dan Informatika dalam meningkatkan kesadaran keamanan informasi ASN dan P3K Pemerintah Kota Makassar
c. Level Kesadaran Keamanan Informasi Pemerintah Kota Makassar merupakan Indikator Sasaran dari Dinas Komunikasi dan Informatika

1.3 Landasan Hukum

a. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
b. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah

Provinsi dan Kabupaten/Kota (Berita Negara Republik Indonesia Tahun 2017 Nomor 758);

c. Peraturan Walikota Makassar Nomor 86 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika (Berita Daerah Kota Makassar Nomor 88 Tahun 2021).

1. 4 Hasil Yang Diharapkan

Tersedianya Dokumen hasil Survey Pengukuran Tingkat Kesadaran Keamanan Informasi di Pemerintah Kota Makassar.

BAB II

TINJAUAN PUSTAKA

2. 1 Konsep Keamanan Informasi

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

1. Phishing

Phishing 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 cara cara 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. Selain itu dalam pesan Spam, terkadang memuat link yang mengarahkan ke situs phising. Sementara kontrol teknis yang diterapkan organisasi untuk

mencegah Spam masuk ke sistem e-mail organisasi mungkin tidak dapat mengatasi 100%. Oleh karena itu, penting baki karyawan atau individu untuk menyadari konsep Spam dan bahaya yang terkait.

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 phishing, password dapat diperoleh secara ilegal dengan menggunakan dua jenis serangan yang dikenal sebagai password cracking. Bukan masalah apakah password dapat dipecahkan atau tidak, melainkan berapa lama waktu 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 dalam sistem tidak boleh memiliki ruang kemungkinan kesalahan.
b. Kepercayaan, memastikan akurasi dan kebenaran akan memastikan bahwa informasi yang 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

2. 2 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, personnel 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 sangat 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 di dalam sebuah aplikasi dan dalam proses kerja mereka. Pelatihan tentang peralatan atau fitur keamanan di dalam 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.

2. 3 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.

Pengukuran dilakukan dengan cara sederhana berdasarkan persentase 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 (Kruger & 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 ke dalam 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:

1. Selalu taat pada aturan perusahaan
2. Menjaga kerahasiaan password dan Personal Identity Number (PIN)
3. Menggunakan e-mail dan internet dengan bijaksana
4. Berhati-hati menggunakan perangkat seluler
5. Melaporkan insiden keamanan informasi,
6. Menyadari konsekuensi setiap tindakan

2. 4 Multi Criteria Decision Making (MCDM)

Multi Criteria Decision Making (MCDM) adalah suatu metode pengambilan keputusan untuk menetapkan alternatif terbaik dari sejumlah alternatif berdasarkan beberapa kriteria tertentu. MCDM memiliki dua kategori yakni Multiple Objective Decision Making (MODM) dan Multiple Attribute Decision Making (MADM). Multiple Objective Decision Making (MODM) adalah suatu metode dengan mengambil banyak kriteria sebagai dasar dari pengambilan keputusan yang didalamnya mencakup masalah perancangan (design), dimana teknik teknik matematik untuk optimasi digunakan dan untuk jumlah alternatif yang sangat besar (sampai dengan tak terhingga). Sedangkan Multiple Attribute Decision Making (MADM) adalah suatu metode dengan mengambil banyak kriteria sebagai dasar pengambilan keputusan, dengan penilaian yang subjektif menyangkut

masalah pemilihan, dimana analisis matematis tidak terlalu banyak dan digunakan untuk pemilihan alternatif dalam jumlah sedikit.

Berikut adalah beberapa penelitian terdahulu tentang pengambilan keputusan untuk masalah multi kriteria khususnya di bidang pemilihan supplier. Chen dan Huang (2007) melakukan penelitian pada Perusahaan Komputer dengan tipe build-to-order (BTO). Belum ada penerapan pembobotan supplier sehingga tidak diketahui supplier mana yang menguntungkan untuk dipilih. Peneliti memadukan metode Analytic Hierarchy Process (AHP) dengan bi-negotiation agents' mechanism untuk membantu memperoleh supplier terbaik pada perusahaan komputer. Penelitian ini mampu mengakomodir kriteria kuantitatif dan kualitatif. Penelitian lain dilakukan oleh Kahraman, dkk (2003) pada sebuah perusahaan white goods di Turki yang bersifat make to order (MTO). Perusahaan ini belum mampu menganalisis supplier yang paling menguntungkan untuk di pilih. Para peneliti menggunakan metode AHP (Analytic Hierarchy Process) dengan kriteria seperti kriteria supplier, kriteria performansi produk, kriteria performansi pelayanan, dan kriteria harga. Teori fuzzy decision-making dapat digunakan untuk membuat suatu keputusan pada lingkungan yang kompleks (multi-criteria). Perçin (2006) juga melakukan penelitian mengenai pemilihan supplier dengan mengintegrasikan AHP (Analytic Hierarchy Process) dan multi objektif PGP (Pre-emptive Goal Programming). Perusahaan yang ditinjau adalah perusahaan otomotif multinasional yang memproduksi airbags, sabuk

pengaman, setir, dan peralatan elektronik untuk keselamatan. Perusahaan hendak menganalisis supplier yang paling menguntungkan untuk dipilih. Dengan memadukan metode antara AHP (Analytic Hierarchy Process) dan multi objektif PGP (Pre-emptive Goal Programming) dapat membantu memperoleh supplier yang lebih menguntungkan.

Chan, dkk (2007) juga melakukan penelitian pada Airline Industry (Hong Kong based- Airline Company). Persaingan dalam industri penerbangan membuat perusahaan ini harus mereduksi biaya-biaya untuk mengurangi biaya pada konsumen, salah satunya adalah dengan meninjau kembali supplier mereka (supplier bahan baku, supplier perbaikan, supplier perawatan) dan memilih yang terbaik dari supplier tersebut. Peneliti menggunakan AHP (Analytic Hierarchy Process) dengan bantuan software Expert Choice. Tujuan dari penelitian ini adalah mengembangkan sebuah pendukung keputusan mengenai pemilihan supplier dengan menggunakan AHP untuk menangani permasalahan mengenai supplier pada airline industry. Penelitian ini memperoleh hasil mengenai supplier terbagus. Software Expert Choice akan menunjukkan supplier dengan bobot tertinggi berdasarkan kriteria-kriteria tersebut. Dewayana dan Budi (2009) melakukan penelitian pada PT. Olex Cables Indonesia (OLEXINDO). Permasalahan yang dihadapi perusahaan adalah terdapat kelemahan dalam pemilihan pemasok yang dilakukan oleh PT. Olexindo yaitu pengambil keputusan hanya menilai berdasarkan pada harga yang ditawarkan dan kualitas yang dimiliki bahan baku secara subyektif.

Penelitian ini bertujuan untuk melakukan pemilihan pemasok dengan pertimbangan yang lebih komprehensif dan objektif sesuai dengan kebutuhan. Metode yang digunakan adalah ANP (Analytic Network Process) dan kriteria yang digunakan adalah kriteria harga, kriteria pengiriman, kriteria kualitas, kriteria pembayaran, kriteria pelayanan.

Triyanti dan Gadis (2008) melakukan analisis pemilihan supplier pada industri makanan. Industri yang diteliti selama ini belum memiliki prosedur pemilihan supplier yang standard, sehingga barang yang dipasok khususnya bahan baku packaging mengalami keterlambatan pengiriman, dan kualitas yang diberikan oleh supplier sering cacat atau rejected. Tujuan dari penelitian ini adalah untuk mengidentifikasikan kriteria yang dipakai dalam pemilihan supplier berikut bobotnya dan juga menentukan urutan performansi dari supplier. Metode yang dipakai adalah penggabungan metode Entropy dan Promethee.

Hidayat (2008) melakukan analisis pemilihan supplier bahan baku daun kayu putih di Pabrik Minyak Kayu Putih (PMKP) Krai, Gundih. Metode yang digunakan adalah Promethee (Preference Ranking Organization Method for Enrichment Evaluation). Kriteria yang digunakan pada penelitian ini adalah kondisi finansial, sumber daya pendukung, kualitas, delivery time, accessibility, responsiveness, dan payment term. Pembobotan kriteria pada penelitian ini dihitung dengan menggunakan metode NGT (Nominal Group Technology). Tujuan dari penelitian ini adalah menentukan kriteria kriteria yang berpengaruh dalam pemilihan supplier dan menentukan prioritas

alternatif supplier bahan baku daun kayu putih. Penelitian sekarang memiliki persamaan dengan penelitian yang dilakukan oleh Hidayat (2008) yakni sama-sama melakukan penelitian untuk menentukan urutan prioritas supplier bahan baku. Penelitian ini dilakukan di Unit Plat (UPL), PT. Mega Andalan Kalasan.

Permasalahan yang dihadapi perusahaan saat ini khususnya pada Unit Plat adalah bahwa prosedur pemilihan supplier pada bahan baku Plat SUS BA (304) 1.0x4”x8” masih terlalu subjektif karena didasarkan pada pengalaman dan hubungan yang telah ada selama ini. Metode yang digunakan adalah Promethee (Preference Ranking Organization Method for Enrichment Evaluation). Kriteria yang digunakan adalah legalitas usaha, pengalaman usaha, kualitas barang, pengiriman, pembayaran, harga, komunikasi. Pembobotan kriteria pada penelitian ini dihitung dengan menggunakan metode Perbandingan Berpasangan. Tujuan penelitian ini adalah untuk mengidentifikasi kriteria yang digunakan pada pemilihan supplier dan memperoleh urutan prioritas supplier bahan baku, sehingga pengambil keputusan dapat mengetahui preferensi supplier yang akan dipilih. Perbedaan penelitian sekarang dengan penelitian terdahulu yang menggunakan metode Promethee adalah pada cara penghitungan bobot kriteria. Perhitungan bobot kriteria yang dilakukan Triyanti dan Gadis (2008) adalah berdasarkan metode NGT (Nominal Group Technology). Perhitungan bobot kriteria yang dilakukan Hidayat (2008) adalah berdasarkan metode NGT (Nominal Group Technology). Sedangkan pada

penelitian sekarang perhitungan bobot berdasarkan metode Perbandingan Berpasangan. Perbedaan lain terdapat pada perbedaan objek, tujuan penelitian, dan kriteria yang digunakan.

BAB III

Metode Penelitian

3. 1 Pendekatan Penelitian

Pendekatan penelitian yang akan digunakan adalah penelitian kuantitatif dengan metode pengumpulan data dengan survei. Survei akan dilaksanakan dengan melakukan wawancara langsung dengan ASN dan PPPK dalam lingkup Pemerintah Kota Makassar menggunakan kuesioner

3. 2 Populasi dan Sampel

Populasi dalam penelitian adalah ASN dan P3K yang bekerja di Pemerintah Kota Makassar. Jumlah sampel akan ditentukan dengan rumus slovin dengan persentase sampling error yang ditolerir 5 %.

$$n = \frac{N}{1 + Ne^2}$$

Dimana:

n = ukuran sampel

N = ukuran populasi

e = kelonggaran ketidaktelitian karena kesalahan pengambilan sampel yang dapat ditoleransi, misalnya 5 %.

Jumlah sampel dengan menggunakan rumus 384,6 tetapi dibulatkan sampai 400 (terlampir). Ketika sudah diketahui jumlah sampel berdasarkan rumus Slovin, maka selanjutnya sampel tersebut akan

didistribusi secara proporsional masing-masing SKPD. Apabila ada SKPD yang mendapatkan jatah sampel di bawah dua maka akan ditambahkan menjadi dua sampel. Sampel tersebut diambil dari SKPD yang jatah sampelnya besar.

Setelah jumlah sampel ditetapkan masing-masing SKPD, penentuan responden akan ditentukan dengan cara *Systematic Random Sampling* terlebih dahulu mengelompokkan responden masing-masing SKPD berdasarkan jenis kelamin.

3. 3 Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 96 pertanyaan dari kesadaran keamanan informasi untuk menguji *attitude, knowledge* dan *behavior* dalam perspektif penggunaan *teknologi* informasi. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu Benar, tidak tahu dan salah (dimensi *attitude* dan *knowledge*), sementara yang lain hanya membutuhkan jawaban yang Benar atau salah (dimensi *behavior*).Pertanyaan yang diajukan dapat dilihat di lampiran

3. 4 Variabel Penelitian

Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang keamanan informasi), Sikap (bagaimana perasaan mereka tentang keamanan informasi), Dan perilaku (apa yang mereka lakukan terhadap keamanan informasi) Masing-

masing dimensi tersebut kemudian terbagi menjadi enam fokus area keamanan informasi yaitu

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

3. 5 Analisis Data

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.

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 MCDM 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) atau sebaliknya perhitungan nilai total masing-masing alternatif (area kesadaran keamanan informasi) yang merupakan jumlah nilai keseluruhan kriteria (dimensi).

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 perhitungan skor kesadaran.

Penentuan bobot untuk masing-masing dimensi pengetahuan, sikap dan perilaku ditentukan berdasarkan skala pembobotan yang digunakan oleh Kruger & Kearney (2005). Pembobotan ketiga dimensi tersebut ditunjukkan pada tabel berikut:

Tabel 3.1 Hasil Pembobotan Masing-Masing Dimensi

No	Dimensi	Bobot
1	Pengetahuan	30
2	Sikap	20
3	perilaku	50

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

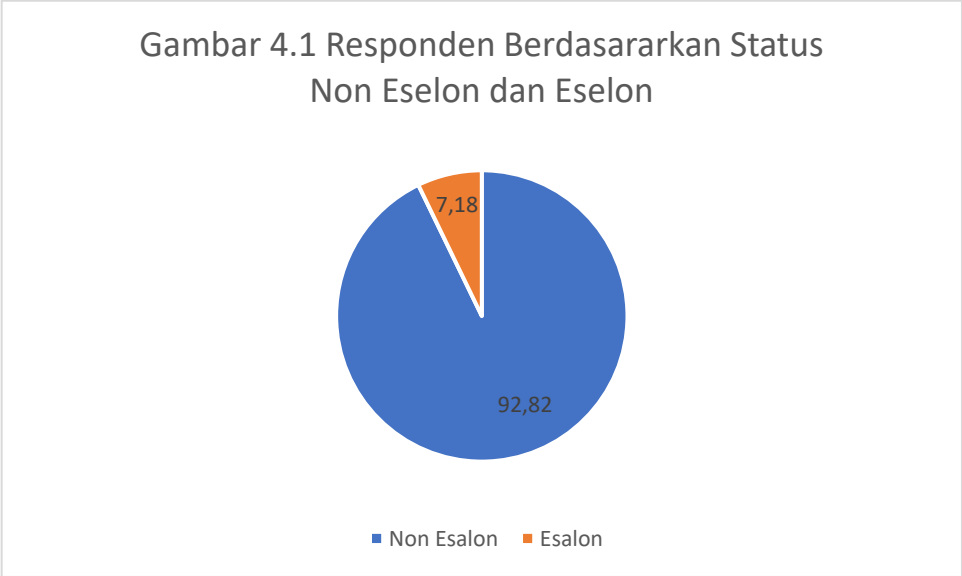
Tabel 3.2 Skala Tingkat Kesadaran dan Keamanan Informasi

NO	Level	Nilai	Keterangan
1	Baik	80 - 100	Tidak Perlu Perbaikan
2	Sedang	60 - 17	Berpotensi ada Perbaikan
3	Buruk	0 - 59	Mutlak ada perbaikan

BAB IV

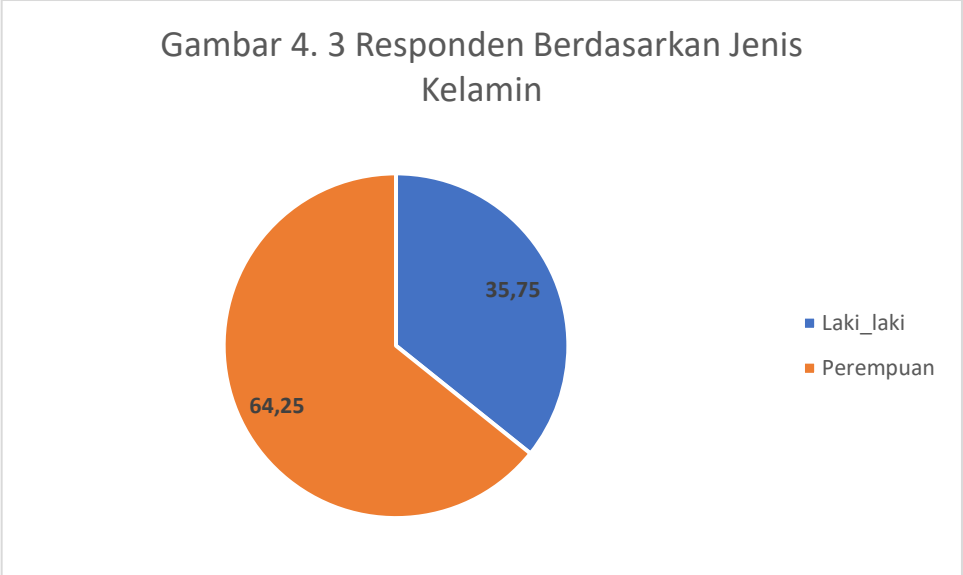
HASIL DAN PEMBAHASAN

4. 1 Karakteristik Responden

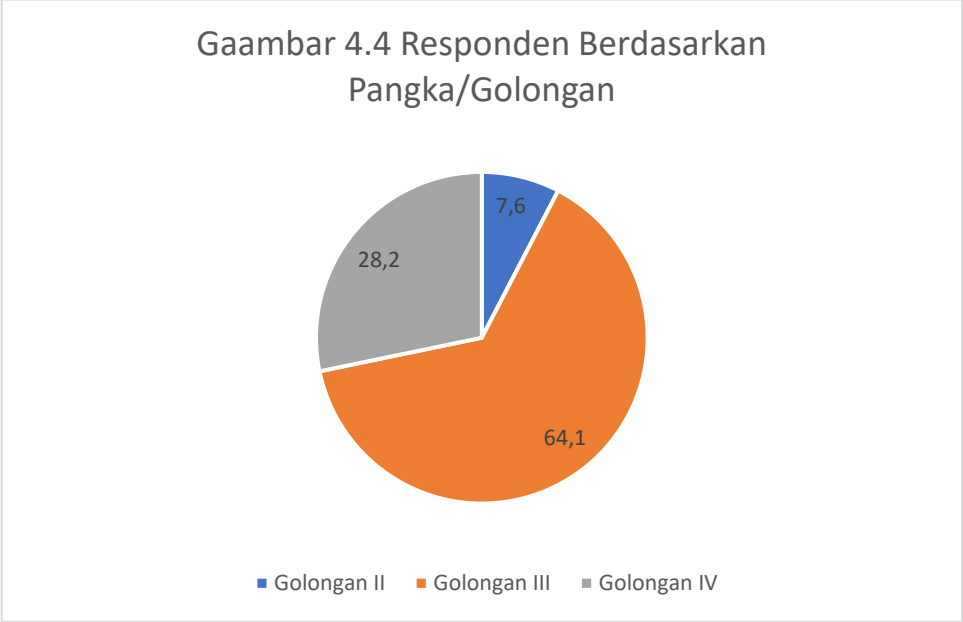


Dari hasil keseluruhan responden berdasarkan status jabatan non eselon dan eselon, terdapat 92,82 % berasal dari pegawai dengan status pejabat non eselon. Sedangkan responden yang berasal dari pejabat eselon sebesar 7,18%.

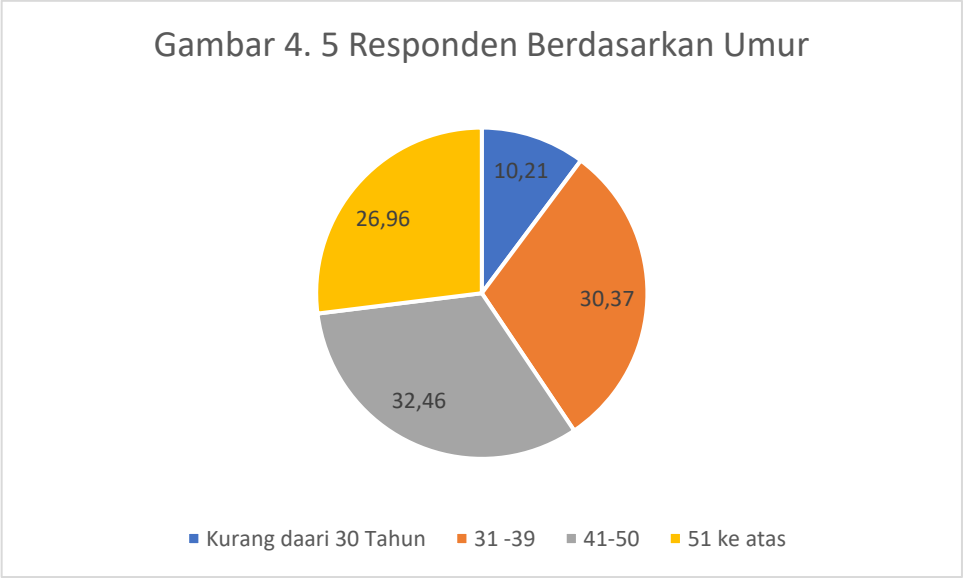
Berdasarkan data di atas, untuk responden pegawai aparatur sipil negara sebesar 90,5 % yang tersebar di 52 SKPD di Kota Makassar. Sedangkan jumlah responden dengan status Pegawai Pemerintah dengan Perjanjian Kerja (P3K) sebesar 9,5%.



Berdasarkan data gambar untuk jenis kelamin responden survey keamanan informasi pegawai pemerintah Kota Makassar, jenis kelamin Laki-laki sebanyak 35,75 %. Sedangkan untuk pegawai berjenis kelamin perempuan ialah 64,25% atau cukup mayoritas.



Dari hasi gambar diagram lingkaran tentang golongan responden, sebanyak 64,1 % dari golongan III atau dominan responden dari golongan ini. Untuk responden dari golongan IV sebesar 28,2 %. Adapun yang dari golongan I hanya sekitar 7,6% atau sangat kecil.



Dari gambar di atas untuk gambaran responden dari segi usia, yang paling besar dari usia 41- 50 tahun yakni 32,46 %. Kemudian untuk usia 31-

39 tahun sebesar 30,37 %, usia 51 tahun ke atas sebanyak 26,96 %. Untuk yang paling rendah jumlah respondennya yakni dari usia kurang dari 30 tahun, hanya 10,21 %.

4.2 Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi

Pengukuran tingkat kesadaran keamanan informasi pegawai Pemerintah Kota Makassar dilakukan dengan melakukan wawancara terhadap 400 responden yang tersebar pada 51 SKPD/OPD. Pegawai yang menjadi sampel adalah ASN dan P3K. Berikut adalah hasil Pengukuran tingkat keamanan informasi. Pembahasan akan diawali dengan melihat tingkat kesadaran keamanan informasi secara umum, kemudian akan dilihat secara spesifik berdasarkan jenis kelamin, umur, kategori kepegawaian dan tempat tugas

Tabel 4.1
Tingkat Kesadaran Keamanan Informasi Pegawai Pemerintah Kota Makassar

Fokus Area	Dimensi (Bobot)			Total
	Pengetahuan (30)	Sikap (20)	Perilaku (50)	
Selalu taat pada aturan perusahaan (policies)	89,2	91,5	90,7	90,4
Menjaga kerahasiaan password dan Personal Identity Number (PIN/password)	90,3	92,7	67,9	79,6
Menggunakan e-mail dan internet dengan bijaksana (email & internet)	74,4	87,8	58,4	69,1
Berhati-hati menggunakan perangkat seluler (mobile equipment)	81,8	87,0	83,0	83,4
Melaporkan insiden keamanan informasi (incidents)	70,4	84,2	65,0	70,5
Menyadari konsekuensi setiap tindakan (consequences)	78,0	94,1	57,5	71,0
Total	80,7	89,5	70,4	77,3

Berdasarkan tabel di atas menunjukkan bahwa bahwa total nilai kesadaran untuk semua dimensi dari semua area yang ada adalah sebesar 77,3 %. Berdasarkan skala tingkatan kesadaran keamanan informasi menunjukkan bahwa dengan hasil tersebut level kesadaran keamanan informasi pegawai dalam lingkup Pemerintah Kota Makassar adalah level sedang atau rata-rata. Hal ini berarti bahwa kesadaran keamanan pegawai dalam lingkup Pemerintah Kota Makassar perlu dimonitor terus karena berpotensi memerlukan tindakan pembenahan. Untuk menunjang tindakan perbaikan ataupun pembenahan perlu dilakukan kegiatan monitoring secara berkelanjutan.

Jika ditinjau dari dimensi-dimensi yang ada, maka dimensi Pengetahuan (*behaviour)* menunjukkan hasil sebesar 70,41 dan merupakan dimensi yang paling rendah serta satu-satunya berada pada level sedang sedangkan dimensi Sikap (*attitude)* dan Perilaku (knowledge) semuanya berada pada level baik. Untuk meningkatkan tingkat kesadaran secara keseluruhan maka dimensi *behaviour* perlu ada peningkatan. Fokus yang perlu ditingkatkan pada dimensi behaviour adalah menggunakan e-mail dan internet dengan bijaksana (email & internet), dan menyadari konsekuensi setiap tindakan (consequences) karena kedua hal tersebut berada pada level buruk.

Jika ditinjau dari masing-masing fokus area, level kesadaran keamanan informasi masuk dalam kategori baik dan sedang. Masuk dalam kategori baik ada dua yaitu selalu taat pada aturan perusahaan (policies),

dan berhati-hati menggunakan perangkat seluler (mobile equipment). Fokus area masuk dalam kategori sedang adalah menjaga kerahasiaan *password* dan Personal Identity Number (PIN/password), melaporkan insiden keamanan informasi (incidents), menyadari konsekuensi setiap tindakan (consequences), dan Menggunakan e-mail dan internet dengan bijaksana (email & internet). Jika masuk dalam kategori baik tidak perlu ada pembenahan sedangkan kategori sedang perlu monitor karena berpotensi membutuhkan pembenahan.

Selalu taat pada aturan perusahaan (policies)

Nilai tingkat kesadaran keamanan informasi pada area selalu taat pada aturan perusahaan (policies) 90,4 masuk dalam kategori baik dalam paling tinggi diantara enam area yang jadi fokus area penelitian. Jika dilihat dari dimensi pengetahuan, sikap dan perilaku nilai tingkat keamanan informasi semuanya masuk dalam kategori baik. Pada area ini Pemerintah Kota Makassar hanya perlu mempertahankan.

Menjaga kerahasiaan password dan Personal Identity Number (PIN/password)

Nilai tingkat kesadaran keamanan dan informasi pada area menjaga kerahasiaan password dan Personal Identity Number (PIN/password) adalah 79,6 masuk dalam kategori sedang. Hal ini berarti bahwa kesadaran keamanan pegawai dalam lingkup Pemerintah Kota Makassar perlu dimonitor terus karena berpotensi memerlukan tindakan pembenahan. Jika dilakukan pembenahan maka berpotensi masuk dalam level baik karena nilainya sudah mendekati 80.

Pada dimensi sikap dan pengetahuan sudah sangat baik karena nilainya di atas 90. Dimensi yang perlu mendapatkan perbaikan adalah pada dimensi pengetahuan karena nilainya masuk dalam kategori sedang dan mendekati angka 60. Masih banyak pegawai dalam lingkup Kota Makassar menggunakan kata sandi dan password yang mudah ditebak, perangkat komunikasi yang digunakan tidak menggunakan *password*, pemberian kata sandi ke pihak lain dan tidak melakukan pergantian PIN/*password* secara berkala. Pada dimensi ini pengetahuan dan sikap yang baik tidak diiringi oleh tindakan yang sesuai.

Menggunakan e-mail dan internet dengan bijaksana (email & internet)

Nilai tingkat kesadaran keamanan dan informasi pada area menggunakan e-mail dan internet dengan bijaksana (email & internet) adalah 69,1 dan masuk dalam kategori sedang. Tingkat kesadaran keamanan dan informasi pada area ini merupakan paling rendah dibandingkan dengan area lainnya. Dari tiga dimensi hanya dimensi sikap masuk dalam kategori baik. Dimensi pengetahuan masuk dalam kategori sedang dan berpotensi untuk diperbaiki agar levelnya bisa naik. Pada dimensi perilaku masuk dalam kategori buruk. Sangat diperlukan tindakan untuk meningkatkan level kesadaran keamanan informasi pada area ini. Untuk meningkatkan kesadaran keamanan informasi perlu ada pemahaman tentang bahaya akses internet dengan menggunakan wifi gratis di tempat umum. Selain itu pemahaman tindakan membuka email dan website yang tidak jelas perlu terus ditingkatkan.

Berhati-hati menggunakan perangkat seluler (mobile equipment)

Nilai tingkat kesadaran dan keamanan informasi berhati-hati menggunakan perangkat seluler (mobile equipment) adalah 83,4 masuk dalam kategori baik. Begitu juga, jika dilihat dari dimensi pengetahuan, sikap dan perilaku semuanya masuk dalam kategori baik sehingga tidak dibutuhkan tindakan mendesak. Meskipun masuk dalam kategori baik tetapi ada satu hal yang perlu mendapatkan perhatian agar tingkat keamanannya meningkat lagi yaitu menggunakan askes internet gratis dengan menggunakan HP di ruang publik untuk transaksi vital seperti mobile banking. Hal yang tergambar pada penjelasan sebelumnya

Melaporkan insiden keamanan informasi (incidents)

Nilai tingkat kesadaran dan keamanan informasi pada area melaporkan insiden keamanan informasi adalah 70,5 dan masuk dalam kategori sedang. Pada dimensi pengetahuan dan perilaku nilainya juga masuk dalam kategori sedang sedangkan sikap masuk dalam kategori baik. Untuk itu perlu ada pembenahan pada dimensi pengetahuan dan terutama dimensi perilaku. Dari dimensi pengetahuan pegawai tidak mengetahui pusat pelaporan jika terjadi kejahatan siber. Kominfo telah menyiapkan Government Computer Security Incident Response team (GOV CSIRT) merupakan layanan layanan untuk meningkatkan keamanan siber tetapi pegawai belum mengetahuinya. Selain itu ciri seseorang yang berniat melakukan kejahatan siber juga belum terpahami dengan baik. Hal tersebut

berdampak kurang nya kasus pelaporan akibat ketidaktahuan mereka tentang informasi dan data yang bisa menimbulkan kejahatan siber.

Menyadari konsekuensi setiap tindakan (consequences)

Berdasarkan pengukuran tingkat kesadaran keamanan informasi area menyadari konsekuensi setiap tindakan (consequences) hasilnya adalah 71,0 dan masuk dalam kategori sedang. Dimensi pengetahuan masuk dalam kategori sedang. Untuk meningkatkan level keamanan informasi pada area ini, maka yang perlu dibenahi adalah sosialisasi tentang phishing karena berpotensi meningkatkan kejahatan siber. Dimensi sikap masuk dalam kategori baik, tidak perlu pembenahan. Dimensi perilaku perlu ada pembenahan karena masuk kategori buruk. Untuk melakukan pembenahan, maka perlu dilakukan adalah sosialisasi kegiatan tentang kejahatan siber. menghindari memperbaiki perangkat komunikasi ke tempat-tempat yang tidak resmi.

Tingkat Kesadaran Keamanan Informasi Berdasarkan Jenis Kelamin

Tabel 4.2
Tingkat Kesadaran Keamanan Informasi Berdasarkan Jenis Kelamin

Fokus Area	Laki-Laki				Perempuan			
	Dimensi			Total	Dimensi			Total
	Pengetahuan (30)	Sikap (20)	Perilaku (50)		Pengetahuan (30)	Sikap (20)	Perilaku (50)	
Selalu taat pada aturan perusahaan (policies)	89,6	92,6	91,7	91,3	88,4	89,5	88,8	88,8
Menjaga kerahasiaan password dan Personal Identity Number (PIN) (password)	90,4	92,4	67,7	79,5	89,9	93,2	68,4	79,8
Menggunakan e-mail dan internet dengan bijaksana (email & internet)	73,4	87,1	61,7	70,3	76,2	89,1	52,7	67,0
Berhati-hati menggunakan perangkat seluler (mobile equipment)	81,4	86,8	83,1	83,3	82,6	87,2	82,8	83,6
Melaporkan insiden keamanan informasi (incidents)	69,5	84,6	65,4	70,5	72,1	83,5	64,2	70,4
Menyadari konsekuensi setiap tindakan (consequences)	76,8	94,9	58,9	71,5	80,2	92,5	55,0	70,1
Total	80,19	89,75	71,41	77,7	81,58	89,17	68,66	76,6

.

Berdasarkan tabel di atas tingkat kesadaran keamanan informasi jenis kelamin laku-laki lebih tinggi dibandingkan dengan perempuan tetapi masih berada pada level yang sama yaitu level sedang. Nilai tingkat kesadaran keamanan informasi laki-laki adalah 77, 7 sedangkan perempuan adalah 76,6. Fokus area yang membuat laki-laki sedikit unggul dibandingkan dengan perempuan adalah menggunakan email dan internet dan bijaksana (email dan internet), dan menyadari konsekuensi setiap tindakan (consequences). Meskipun secara pengetahuan perempuan lebih unggul tetapi dalam hal perilaku justru laki-laki lebih baik. Aktivitas seperti berbelanja dengan menggunakan wifi ruang publik menjadi salah satu tingkat kerawanan yang dimiliki oleh perempuan.

Tabel 4.3
Tingkat Kesadaran Keamanan Informasi Antara ASN dan P3K

Fokus Area	ASN				P3K			
	Dimensi			Total	Dimensi			Total
	Pengetahuan (30)	Sikap (20)	Perilaku (50)		Pengetahuan (30)	Sikap (20)	Perilaku (50)	
Selalu taat pada aturan perusahaan (policies)	89,1	91,3	90,6	90,3	90,7	95,5	94,2	93,4
Menjaga kerahasiaan password dan Personal Identity Number (PIN) (password)	90,2	92,8	68,1	79,7	92,9	94,9	69,2	81,4
Menggunakan e-mail dan internet dengan bijaksana (email & internet)	74,0	88,2	57,7	68,7	76,8	85,5	64,8	72,5
Berhati-hati menggunakan perangkat seluler (mobile equipment)	81,8	86,5	82,6	83,2	83,5	92,5	87,4	87,2
Melaporkan insiden keamanan informasi (incidents)	70,2	84,3	65,2	70,5	76,4	85,3	65,1	72,5
Menyadari konsekuensi setiap tindakan (consequences)	77,9	94,0	57,1	70,7	81,5	97,2	63,1	75,4
Total	80,52	89,52	70,24	77,2	83,63	91,81	73,96	80,4

Berdasarkan tabel di atas tingkat kesadaran keamanan informasi ASN lebih rendah dibandingkan dengan P3K. Nilai tingkat kesadaran ASN

adalah 77,2 masuk dalam kategori sedang, sedangkan P3K 80,4 masuk dalam kategori baik. P3K lebih unggul semua dimensi

Tabel 4.4
Tingkat Kesadaran Keamanan Informasi Berdasarkan Umur

Fokus Area	Umur Di Aatas 40 Tahun				Umur Kurang 40 Tahun			
	Dimensi			Total	Dimensi			Total
	Pengetahuan (30)	Sikap (20)	Perilaku (50)		Pengetahuan (30)	Sikap (20)	Perilaku (50)	
Selalu taat pada aturan perusahaan (policies)	88,2	90,5	90,2	89,7	90,6	93,5	91,6	91,7
Menjaga kerahasiaan password dan Personal Identity Number (PIN) (password)	89,1	91,6	66,5	78,3	91,9	94,7	70,1	81,6
Menggunakan e-mail dan internet dengan bijaksana (email & internet)	70,4	87,0	59,9	68,5	79,8	89,2	58,0	70,8
Berhati-hati menggunakan perangkat seluler (mobile equipment)	80,8	86,3	82,2	82,6	83,9	88,4	84,9	85,3
Melaporkan insiden keamanan informasi (incidents)	70,7	83,8	65,7	70,8	71,4	85,6	64,9	71,0
Menyadari konsekuensi setiap tindakan (consequences)	77,6	95,0	57,6	71,1	79,3	94,0	58,1	71,6
Total	79,48	89,04	70,34	76,8	82,82	90,89	71,27	78,7

Hasil pengukuran tingkat keamanan informasi pada tabel di atas menunjukkan bahwa pegawai yang berumur kurang dari 40 tahun lebih baik dari pada umur di atas 40 tahun, meskipun berada pada level yang sama, yaitu sedang. Keunggulan dari umur kurang 40 tahun karena unggul dari dimensi pengetahuan, sikap dan perilaku. Baik yang berumur kurang dari 40 tahun dan lebih 40 tahun, masing-masing mempunyai nilai tingkat keamanan informasi masuk dalam kategori rendah. Kedua hal tersebut memerlukan tindakan untuk meningkatkan level keamanan informasi paling tidak pada level sedang

Tabel 4.5
Tingkat Kesadaran Keamanan Informasi Berdasarkan Bidang Pekerjaan

Fokus Area	Pegawai OPD Lainya				Pegawai Bidang Pendidikan				Pegawai Kecamatan				Pegawai Bidang Kesehatan			
	Dimensi				Dimensi				Dimensi				Dimensi			
	Pengetahuan (30)	Sikap (20)	Perilaku (50)	Total	Pengetahuan (30)	Sikap (20)	Perilaku (50)	Total	Pengetahuan (30)	Sikap (20)	Perilaku (50)	Total	Pengetahuan (30)	Sikap (20)	Perilaku (50)	Total
Selalu taat pada aturan perusahaan (policies)	88,2	90,5	87,8	88,50	90,6	93,3	91,6	91,6	83,2	90,2	90,2	88,1	90,5	88,5	93,4	91,5
Menjaga kerahasiaan password dan Personal Identity Number (PIN/password)	89,2	89,0	63,8	76,42	91,3	94,2	69,8	81,1	90,3	93,9	58,4	75,0	88,1	93,3	76,3	83,2
Menggunakan e-mail dan internet dengan bijaksana (email & internet)	73,3	83,9	53,9	65,68	73,9	89,2	62,2	71,1	75,0	89,0	49,1	64,9	76,9	89,2	58,7	70,3
Berhati-hati menggunakan perangkat seluler (mobile equipment)	81,8	83,4	82,3	82,38	81,4	88,7	82,5	83,4	82,9	85,5	83,6	83,8	82,7	87,7	86,1	85,4
Melaporkan insiden keamanan informasi (incidents)	63,4	76,6	63,0	65,86	74,9	88,3	66,8	73,5	67,0	82,1	60,5	66,8	70,6	85,9	67,2	72,0
Menyadari konsekuensi setiap tindakan (consequences)	74,2	91,3	56,2	68,61	80,0	96,0	58,9	72,6	76,3	93,4	55,1	69,1	79,8	93,1	57,5	71,3
Total	78,35	85,78	67,83	74,58	82,05	91,62	71,96	78,92	79,14	89,01	66,13	74,61	81,44	89,61	73,18	78,95

Tabel di atas adalah perbandingan tingkat keamanan informasi antara pegawai yang bertugas di Kantor Kecamatan, bidang Pendidikan, bidang kesehatan dan OPD lainnya. Pegawai bidang pendidikan yang dimaksud adalah pegawai yang bekerja di Dinas Pendidikan dan Guru sedangkan bidang kesehatan adalah pegawai yang bekerja di Dinas Kesehatan, Puskesmas dan RSUD. OPD lainnya yang dimaksud adalah diluar dari ketiga kategori lainnya.

Berdasarkan hasil Pengukuran tingkat kesadaran keamanan informasi semuanya berada pada level baik, tetapi nilai berbeda. Pegawai yang bertugas di bidang pendidikan dan kesehatan lebih tinggi dibandingkan dengan pegawai yang bertugas di Kantor Kecamatan dan OPD lainnya. Paling tinggi nilainya adalah pegawai yang bertugas di bidang kesehatan tetapi hanya unggul tipis dibandingkan dengan bidang

Pendidikan, sedangkan paling rendah adalah OPD lainnya tetapi nilainya hampir sama dengan pegawai di Kantor Kecamatan.

Keempat pengelompokan tersebut di atas masing-masing punya nilai tingkat kesadaran keamanan informasi berada pada level rendah. Jika dilihat dari sisi dimensi, level rendah tersebut semuanya berada pada dimensi pengetahuan. Pada OPD lainnya area yang berada pada level rendah adalah menggunakan e-mail dan internet dengan bijaksana (email & internet), dan menyadari konsekuensi setiap tindakan (consequences). Hal yang sama terjadi juga pada bidang kesehatan. Bidang Pendidikan hanya punya satu area berada pada level bawah yaitu menggunakan e-mail dan internet dengan bijaksana (email & internet). Pegawai bertugas di Kantor Kecamatan paling banyak berada pada level rendah. Area yang berada pada level rendah adalah menggunakan e-mail dan internet dengan bijaksana (email & internet), dan menyadari konsekuensi setiap tindakan (consequences), dan menjaga kerahasiaan password dan Personal Identity Number (PIN/password)

BAB V

Kesimpulan dan Rekomendasi

5. 1. Kesimpulan

1. Tingkat kesadaran keamanan informasi pegawai Pemerintah Kota Makassar berada pada level sedang dengan nilai 77,3
2. Tingkat kesadaran keamanan informasi pegawai Pemerintah Kota Makassar dari sisi dimensi Pengetahuan (*knowledge)* dan Sikap (*Attitude)* masuk dalam kategori baik sedangkan dari sisi dimensi perilaku (*Behaviour*) masuk dalam kategori sedang
3. Tingkat kesadaran keamanan informasi pegawai Pemerintah Kota Makassar dari sisi fokus area masuk dalam level baik adalah selalu taat pada aturan perusahaan (policies), dan berhati-hati menggunakan perangkat seluler (mobile equipment) sedangkan masuk dalam level sedang adalah selalu taat pada aturan perusahaan (policies), menjaga kerahasiaan password dan Personal Identity Number (PIN/password), menggunakan e-mail dan internet dengan bijaksana (email & internet), berhati-hati menggunakan perangkat seluler (mobile equipment), melaporkan insiden keamanan informasi (incidents), dan menyadari konsekuensi setiap tindakan (consequences)

4. Tingkat kesadaran keamanan informasi dari dimensi perilaku paling rendah nilainya dan terdapat dua fokus area level rendah sehingga mutlak untuk dibenahi.
5. Tingkat kesadaran keamanan informasi dari dimensi pengetahuan meskipun masuk dalam kategori baik tetapi masih tetap perlu ada pembenahan karena separuh fokus area masuk dalam kategori sedang
6. Tingkat kesadaran keamanan informasi di dimensi sikap nilai cukup tinggi dan berada pada level baik sehingga tidak perlu ada perbaikan.

5.2 . Rekomendasi

1. Secara umum kesadaran keamanan informasi pegawai pemerintah Kota Makassar berada pada level sedang sehingga masih perlu dimonitor terus karena berpotensi memerlukan tindakan pembenahan
2. Dimensi yang perlu mendapatkan perhatian adalah dimensi pengetahuan dan perilaku. Meskipun dimensi pengetahuan masuk dalam kategori baik tetapi ada sejumlah area yang masih membutuhkan pembenahan
3. Dimensi pengetahuan yang perlu ada pembenahan adalah:
    a. Meningkatkan pengetahuan untuk mengidentifikasi kegiatan atau gerak gerik seseorang yang berpotensi melakukan kejahatan internet

b. Akses internet dengan menggunakan jaringan di tempat umum (Wifi gratis) merupakan tindakan berbaya terutama mobile banking

c. Sosialisasi keberadaan Government Computer Security Incident Response team (GOV CSIRT) dari Kementerian Kominfo merupakan layanan layanan untuk meningkatkan keamanan siber

d. Meningkatkan pengetahuan agar terhindar dari kejahatan dari kemajuan teknologi informasi (kejahatan siber) seperti email berbaya, website berbaya dan kegiatan *Phishing*

e. penggunaan WiFi publik (gratis) untuk mengakses mobile banking atau transaksi penting lainnya sebaiknya dihindari

f. Menggunakan password yang sama untuk akses akun atau perangkat merupakan tindakan berbahaya

g. Memperbaiki perangkat komunikasi (komputer, Laptop, dan HP) yang yang rusak kepada tukang service bisa berakibat bocornya data informasI

4. Dimensi Perilaku yang perlu dilakukan agar level kesadaran keamanan informasi semakin meningkat adalah

   a. Memperbaiki perangkat komunikasi (computer, Laptop, dan HP) tempat yang resmi.

   b. Komputer/laptop yang biasa saya pakai harus mempunyai anti virus update

c. Menghindari akses internet menggunakan data gratis tersedia di ruang public

d. Mengikuti secara aktif kegiatan sosialisasi terhindar dari kejahatan akibat kemajuan teknologi (kejahatan siber) baik secara during maupun luring

e. Menghindari transaksi perbankan atau transaksi penting lainnya dengan wifi publik (gratis)

f. tidak membuka email yang dikirimkan meskipun saya tidak mengenal pengirimnya

g. Tidak memberikan informasi atau data tentang pekerjaan kepada pihak lain yang mendapat persetujuan atasan

h. Mencari informasi tentang Government Computer Security Incident Response team (GOV CSIRT) merupakan layanan layanan untuk meningkatkan keamanan siber

i. Tidak memberi tahu kata sandi/ password kepada orang yang lain

j. Tidak mengunduh (download) file pada situs (web) tanpa memperhatikan keasliannya atau berbahaya bagi perangkat komunikasi dan data

k. Perangkat lunak yang diinstal pada perangkat komunikasi (computer/laptop/HP) yang biasa saya pakai haris original

l. Tidak Menggunakan password sama untuk berbagai keperluan dan selalu mengganti password/PIN secara berkala

m. Semua perangkat komunikasi, akun, media sosial, yang biasa saya gunakan menggunakan password

n. Selalu memusnahkan hasil cetakan/data sifatnya penting/rahasia

o. Menghindari password/PIN yang mudah ditebak seperti nama sendiri, tanggal lahir, angka berurutan, atau angka berulang

p. Selalu memastikan akses web atau interaksi dari pihak lain aman dari kegiatan phishing

q. Jangan memberikan email untuk digunakan orang lain atau pihak ketiga

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 assessing information security awareness. Computer & Security, 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 Rotterdam.

Priandoyo, A. (2006). Vulnerability Assessment 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.

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

LAMPIRAN