Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa

Dafid*[1], Dorie[2]
[1]Universitas Sriwijaya; Jl. Srijaya Negara, Telp:(0711)379249
[1]Program StudiDoktor Ilmu Teknik, FTeknikUNSRI, Palembang
[1,2]STMIK GI MDP; Jl. Rajawali No.14, Telp:(0711)379249
[1,2]Program StudiSistem Informasi, STMIK GI MDP, Palembang
e-mail: *[1]dafid@mdp.ac.id,[2]dpkesuma@staff.mdp.ac.id

Abstrak

Pada sebuah institusi pendidikan tinggi tentunya hal yang lumrah dilakukan oleh mahasiswa dalam menjalankan berbagai aktifitas akademik dan non akademik dengan memanfaatkan teknologi informasi. Kesadaran akan keamanan informasi merupakan salah satu faktor penting didalam pemanfaatan teknologi tersebut. Tingkat kesadaran yang rendah akan mengakibatkan banyaknya insiden keamanan informasi yang muncul. Penelitian ini melakukan pengukuran tingkat kesadaran mahasiswa STMIK XYZ terhadap keamanan informasi. Tujuan penelitian ini untuk mengetahui tingkat kesadaraan keamanan informasi mahasiswa dengan demikian dapat ditentukan tindakan yang perlu dilakukan untuk memperbaiki kesadaran yang masih rendah dan mempertahankan yang sudah baik. Metode yang digunakan adalah metode Multiple Criteria Decision Analysis (MCDA). Metode pengumpulan data menggunakan kuesioner. Hasil penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi mahasiswa STMIK XYZ berada pada level "sedang" dengan nilai 71%. Dari tiga dimensi yang diukur hanya ada satu dimensi yang berada pada level "buruk" yaitu dimensi behaviour. Dari enam area pengukuran ada tiga area pengukuran yang berada pada level buruk yaitu policies, mobile equipment dan consequences. Hasil tersebut menunjukkan perlu adanya perhatian khusus dan tindakan konkrit untuk meningkatkan level kesadaran keamanan informasi.

Kata kunci*—keamanan informasi , level kesadaran, MCDA*

Abstract

In a higher education institution, it is certainly common for students to carry out various academic and non-academic activities using information technology. Awareness of information security is one of the substantial factors in the utilization of these technologies. With low level of awareness, information security incidents will be arising. This research measures the level of information security awareness of STMIK XYZ students. The purpose of this researchis to determine the level of information security awareness of students so that actions can be determined that need to be taken to improve low awareness and maintain what is already good. This research using Multiple Criteria Decision Analysis (MCDA) method. The results showed that information security awareness's level of STMIK XYZ students is "average" (score: 71%). From three dimensions that measured, there is only one dimension that at "poor"level (behavior dimension).From six measurement areas, three measurement areas; policies, mobile equipment, and consequences are at a poor level. These results indicate that some actions required to improve information security awareness's level of STMIK XYZ students.

Keywords*—information security, awareness level, MCDA*

1. PENDAHULUAN

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 di manapun kita berada. Perkembangan Teknologi informasi telah masuk ke seluruh sendi kehidupan manusia salah satunya adalah dalam bidang pendidikan yaitu di kalangan para mahasiswa. Banyak aktifitas mahasiwa yang dilakukan berhubungan dengan teknologi informasi. Baik itu aktifitas 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 *scaning* 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 *Avaibility*. *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. *Avaibility* adalah menjamin informasi dapat diakses kapanpun oleh pemilik atau pengguna informasi tanpa terjadi gangguan atau perubahan informasi tersebut. Perlu kesadaran yang tinggi bagi para mahasiswa dalam memanfaatkan teknologi informasi tersebut.

Hasil penelitian sebelumnya yang dilakukan oleh [1] menunjukkan bahwa tingkat kesadaran keamanan informasi pada pegawai pemerintahan secara keseluruhan berada pada level sedang sehingga perlu dimonitor untuk kemungkinan dilakukan pembenahan. Penelitian tersebut menggunakan metode MCDA. Hal ini tentu saja belum tentu mencerminkan tingkat kesadaran pengguna layanan IT secara umum sehingga perlu ada penelitian untuk objek yang berbeda. Penelitian lain yang dilakukan oleh [2] dilakukan dengan menggunakan metode eksperimental terhadap pengguna *e-learning* pada institusi perguruan tinggi. Objek penelitian tersebut adalah mahasiswa namun hanya berfokus pada layanan *e-learning* saja dimana hasil penelitian menunjukkan bahwa tingkat kesadaran mahasiswa terhadap keamanan sistem e-learning masih lemah. Penelitian ini melengkapi penelitian sebelumnya dengan menggunakan metode MCDA yang mana dari hasil penelitian ini diharapkan dapat meningkatkan kesadaran pengguna IT secara umum dan pihak terkait untuk mengambil langkah-langkah yang diperlukan dalam rangka memperbaiki dan meningkatkan kualitas keamanan layanan IT.

2. TINJAUAN PUSTAKA

Berikut ini akan dijabarkan beberapa definisi/teori yang digunakan dalam penelitian ini.

2.1 Metode Pengumpulan Data

Observasi sebagai teknik pengumpulan data mempunyai ciri yang spesifik bila dibandingkan dengan teknik yang lain, yaitu wawancara dan kuesioner. Jika wawancara dan kuesioner selalu berkomunikasi dengan orang, maka observasi tidak terbatas pada orang, tetapi juga pada obyek-obyek alam yang lain juga [3]. Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab. Kuesioner merupakan teknik pengumpulan data yang efisien bila peneliti tahu dengan pasti variabel yang akan diukur dan tahu apa yang diharapkan dari responden. Selain itu kuesioner juga sangat cocok untuk digunakan jika jumlah responden cukup besar dan tersebar di wilayah yang luas.

2.2 Keamanan Informasi

Menurut McLeod dan Schell [4] keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu kerahasiaan, ketersediaan dan integritas. Menurut Whitman dan Mattord [5] keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut Whitmandan Mattord [5], *Security Awareness* adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadap keamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan. Menurut Kruger & Kerney [6], menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni *cognition, affection dan behaviour*. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *Knowledg*e (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behavio*ur (perilaku seseorang). Kruger melakukan pengukuran pada ketiga dimensi ini di 6 area yang termasuk memiliki resiko yang kritis yaitu:

a. Selalu taat pada aturan perusahaan (*policies*-A1)
b. Menjaga kerahasiaan password dan *Personal Identity Number (PIN)* (*password*-A2)
c. Menggunakan e-mail dan internet dengan bijaksana (*email* &*internet*-A3)
d. Berhati-hati menggunakan perangkat seluler (*mobile equipment*-A4)
e. Melaporkan insiden keamanan informasi (*incidents*-A5)
f. Menyadari konsekuensi setiap tindakan (*consequences*-A6)

2.3 Metode Multiple Criteria Decision Analysis (MCDA)

Metode *Multiple Criteria Decision Analysis (MCDA)* biasanya digunakan untuk mengambil keputusan atas beberapa alternatif yang memiliki banyak kriteria. Metode *Multiple Criteria Decision Analysis* digunakan untuk mengukur nilai total *alternative* berdasarkan kriteria-kriteria tertentu. Pendekatan MCDA dibedakan menjaditiga kategori [7] yaitu:

1. *Value measurement model*
2. Model perangkingan
3. *Goal programming*

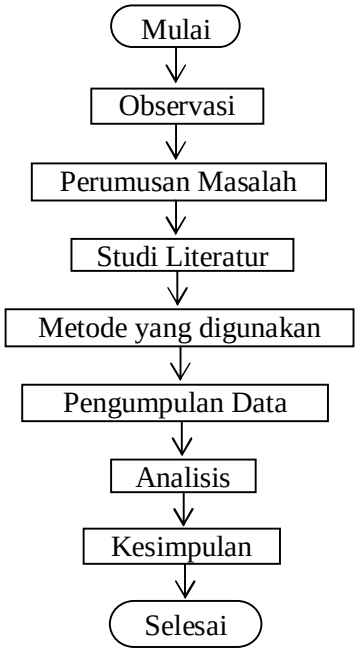
Secara matematis, pendekatan motode *Multiple Criteria Decision Analysis (MCDA*) ditunjukkan pada persamaan berikut:

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

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

3. METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan penelitian dengan menggunakan metode-metode tertentu. Adapun tahapan-tahapan penelitian yang dilakukan dapat dilihat pada gambar 1. Tahapan penelitian dimulai dari observasi untuk selanjutnya akan menghasilkan rumusan masalah (*problem statement*). Selanjutnya dilakukan studi literatur terkait *problem statement* yang telah ditentukan baik yang bersumber dari buku, jurnal maupun publikasi ilmiah lainnya. Dari studi literatur yang dilakukan dapat diidentifikasi metode-metode yang dapat digunakan untuk menyelesaikan masalah tersebut. Untuk memudahkan dalam melakukan analisa dan pengolahan data maka terlebih dahulu dilakukan pengumpulan data. Tahap akhir dari penelitian ini adalah penarikan kesimpulan dari pembahasan yang dilakukan.



Gambar 1. Metode Penelitian

Pada gambar 1 diatas dapat dijelaskan sebagai berikut:

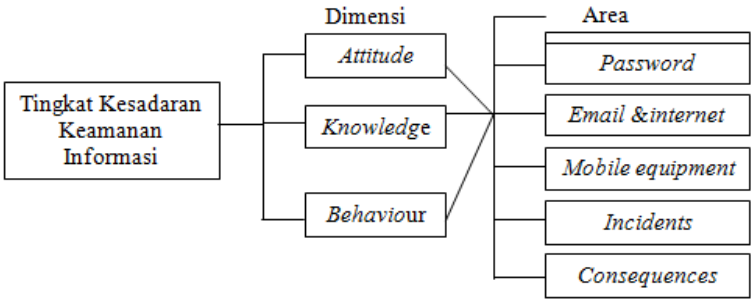
1. Kegiatan penelitian dimulai dengan melakukan pengamatan (observasi) terhadap kegiatan yang berhubungan dengan penggunaan layanan IT yang digunakan oleh mahasiswa di STMIK XYZ dan mengidentifikasi aplikasi atau sistem informasi yang terkait dengan kegiatan tersebut. Dari hasil pengamatan diketahui kegiatan yang dimaksud seperti akses ke sistem/aplikasi menggunakan otorisasi dan otentikasi (*login*) terutama sistem yang berkaitan dengan akademik, pengelolaan pesan (kirim/terima email) maupun penggunaan *social media*.
2. Setelah mendapatkan objek penelitian selanjutnya dilakukan perumusan masalah dengan cara mengidentifikasi masalah-masalah yang selama ini ditemui oleh mahasiswa sehubungan dengan pemanfaatan dari layanan IT yang digunakan. Dari hasil identifikasi selanjutnya permasalahan tersebut dikelompokkan lagi menjadi satu pokok bahasan utama yaitu berkaitan dengan kesadaran (*awareness*) keamanan informasi.

3. Berdasarkan masalah yang telah ditentukan langkah berikutnya adalah pencarian referensi ataupun tinjauan pustaka terhadap penelitian yang akan dilakukan serta dengan melakukan kajian terhadap literatur/penelitian yang pernah dilakukan sebelumnya oleh peneliti-peneliti lain. Dengan demikian dapat memperkaya hasil penelitian sebelumnya dan meningkatkan hasil penelitian yang sedang dilakukan.
4. Setelah melakukan studi literatur didapatkan beberapa metode dengan berbagai versi yang berhubungan dengan masalah kesadaran (*awareness*) keamanan informasi. Dari beberapa metode tersebut ada yang telah digunakan pada penelitian sebelumnya untuk objek dan subjek penelitian yang sama. Melalui kajian secara mendalam dari berbagai metode yang ada ditetapkan untuk penelitian ini menggunakan metode *MULTIPLE CRITERIA DECISION ANALYSIS (MCDA)*. Metode ini dipilih karena sangat mewakili untuk pengukuran kesadaran keamanan informasi yang mencakup enam area pengukuran dalam *prototyp*e yang diperkenalkan oleh [3]. Pengukuran dilakukan berdasarkan persepsi pengguna akhir. Ada 3 dimensi yang digunakan yaitu *Knowledge* (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behaviour* (perilaku seseorang).
5. Untuk mendapatkan hasil penelitian dengan menggunakan metode *MULTIPLE CRITERIA DECISION ANALYSIS (MCDA)* terlebih dahulu dilakukan pengumpulan data dengan menggunakan metode kuesioner. Menurut Sugiyono, populasi adalah wilayah generalisasi yang terdiri atas obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya [8]. Populasi yang digunakan di dalam penelitian ini adalah mahasiswa dari program studi Sistem Informasi, Teknik Informatika dan Manajemen Informatika dari angkatan 2016 hingga 2018 yang ada di STMIK XYZ sebanyak 684 orang. Sedangkan untuk sampel, menurut Sekaran merupakan sebagian dari populasi [9]. Perhitungan untuk menentukan jumlah responden dalam penelitian ini menggunakan rumus perhitungan dari Slovin dengan rumus sebagai berikut: (dengan nilai *margin of error (e)* sebesar 0.05)

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

$$n = \frac{684}{1 + 684 * 0.05^2} = 252.3$$

Dengan demikian dari hasil perhitungan didapatkan jumlah sampel untuk penelitian ini sebesar 252 orang mahasiswa. Pengisian kuesioner dilakukan oleh mahasiswa secara *online* dengan menggunakan *Google Form* pada periode waktu tertentu. Mahasiswa diberikan alamat *website* yang harus mereka akses yang selanjutnya selesai pengisian data akan submit ke server penelitian. Adapun mengenai konsep pertanyaan yang diajukan mengacu kepada kerangka pengukuran kesadaran keamanan informasi yang diperkenalkan oleh Krugger & Kerney. Tingkat kesadaran keamanan informasi mahasiswa ini diukur berdasarkan dimensi *Knowledg*e (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behavio*ur (perilaku seseorang) untuk setiap area mulai dari area *policies, password, email* &*internet, mobile equipmentincidents* sampai *consequences*. Konsep pengukurannya dapat dilihat pada gambar 2 berikut ini:



Gambar 2. Konsep Pengukuran

Untuk menguji *Knowledg*e (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behavio*ur (perilaku seseorang) responden berkaitan dengan tujuh area kesadaran keamanan informasi disusunlah pertanyaan sebanyak 35 buah. Setiap pertanyaan diberikan jawaban dengan 3 skala: benar, tidak tahu dan salah. Pertanyaan itu sendiri digunakan untuk menghitung nilai $v_i(a)$. Adapun contoh pertanyaan yang dimaksud dalam dilihat berturut-turut pada tabel 1, tabel 2 dan tabel 3 berikut ini:

Tabel 1. Contoh Pertanyaan untuk Dimensi *Knowledg*e

Dimensi *Knowledg*e (pengetahuan seseorang)

NO	PERTANYAAN	KETERANGAN		
		Benar	Salah	Tidak tahu
1	Akses internet pada perguruan tinggi adalah sumber daya perguruan tinggi dan hanya boleh digunakan untuk kepentingan pendidikan saja			

Tabel 2. Contoh Pertanyaan untuk Dimensi *Attitude*

Dimensi *Attitude* (sikap seseorang)

NO	PERTANYAAN	KETERANGAN		
		Benar	Salah	Tidak tahu
1	Perangkat seluler biasanya diproteksi dengan perlindungan asuransi dan tidak perlu adanya kebutuhan khusus untuk menyertakannya ke dalam kebijakan keamanan			

Tabel 3. Contoh Pertanyaan untuk Dimensi *Behaviour*

Dimensi *Behavio*ur (perilaku seseorang)

NO	PERTANYAAN	KETERANGAN		
		Benar	Salah	Tidak tahu
1	Saya sadar bahwa saya seharusnya tidak memberikan *password* saya kepada orang lain, namun terkadang pekerjaan /tugas saya pada saat tertentu bisa saja menyebabkan saya harus memberikan *password* saya kepada teman saya (hanya untuk teman yang saya percayai)			

Setelah memperoleh nilai v_i (a) dari kuesioner maka langkah selanjutnya adalah dengan melakukan perhitungan perkalian dengan bobot w_i. Bobot w_i ditentukan dengan menggunakan*Analytic Hierarchy Process (AHP)*. Menurut [1] AHP adalah teoripengukuran menggunakan perbandingan berpasangan dan bergantung pada penilaian ahli untuk

memperoleh skala prioritas. 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. Menurut [1] 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. Penentuan bobot [6] untuk tiap dimensi pengetahuan, sikap dan perilaku ditentukan berdasarkan skala pembobotan yang digunakan oleh Kruger & Kerney [6] dapat dilihat pada tabel 4 berikut ini:

Tabel 4. Bobot Dimensi

Dimensi	**Bobot**
Pengetahuan	30
Sikap	20
Perilaku	50

Sebelum ditentukan level kesadaran keamanan informasi sebagai hasil akhir, untuk proses perhitungan total skor untuk tiap dimensi per area yang telah disebutkan pada bagian sebelumnya dapat dilihat pada tabel berikut ini:

Tabel 5. Perhitungan Total Nilai

Dimensi	**Area**						**Total Nilai**
	A1	**A2**	**A3**	**A4**	**A5**	**A6**	
*Knowledg*e	A11	A21	A31	A41	A51	A61	$\sum_{i=1}^{6} Ai1$ / 6
Attitude	A12	A22	A32	A42	A52	A62	$\sum_{i=1}^{6} Ai2$ / 6
Behaviour	A13	A23	A33	A43	A53	A63	$\sum_{i=1}^{6} Ai3$ / 6
Total Nilai	$\sum_{i=1}^{3} A1i$ / 3	$\sum_{i=1}^{3} A2i$ /3	$\sum_{i=1}^{3} A3i$ /3	$\sum_{i=1}^{3} A4i$ /3	$\sum_{i=1}^{3} A5i$ /3	$\sum_{i=1}^{3} A6i$ /3	

Pada tahap akhir perhitungan akan ditentukan level dari kesadaran keamanan informasi mahasiswa. Level ini mengacu kepada nilai yang telah ditetapkan oleh [6] yaitu baik, sedang dan buruk. Masing-masing level memiliki nilai *range* tersendiri yang dapat dilihat pada tabel 6 berikut ini:

Tabel 6. Level Kesadaran Keamanan Informasi

Hasil Pengukuran (%)	Level
80–100	Baik
60–79	Sedang
59 kebawah	Buruk

4. HASIL DAN PEMBAHASAN

Karakteristik responden merupakan gambaran dari keberadaan responden yang terlibat yaitu program studi. Berdasarkan data deskriptif yang menjelaskan distribusi program studi responden dapat diketahui bahwa responden dari program studi Sistem Informasi sebanyak 122 orang dengan persentase 48.41%, program studi Teknik Informatika sebanyak 100 orang dengan persentase 39,68% dan dari program studi Manajemen Informatika sebanyak 30 orang dengan persentase 11,91% dari jumlah keseluruhan responden sebanyak 252 orang. Data deskriptif tersebut dapat dilihat pada tabel 7 dibawah ini.

Tabel 7. Distribusi Program Studi Responden

Program Studi	Jumlah	Persentase (%)
Sistem Informasi	122	48,41
Teknik Informatika	100	39.68
Manajemen Informatika	30	11.91
Total	252	100

Persentase responden program studi Sistem Informasi sebesar 48.41% menunjukkan bahwa sebagian besar responden adalah berasal dari program studi Sistem Informasi. Untuk hasil perhitungan pembobotan untuk setiap area dengan menggunakan AHP didapat nilai sebagai berikut:

Tabel 8. Hasil Pembobotan

Area	Hasil W_i
Policies	0.478
Password	0.574
Email &internet	0.315
Mobile equipment	0.243
Incidents	0.046
Consequences	0.212

Dari tabel 8 diketahui bahwa area *Password* menunjukkan nilai yang paling maksimum. Hal ini menunjukkan bahwa hal tersebut dapat dikarenakan pemberi pertimbangan lebih menekankan pada aspek menjaga kerahasiaan *password* dan *Personal Identity Number (PIN)*. Dengan menggunakan rumus (1) maka hasil perhitungan level kesadaran keamanan informasi untuk dimensi *Knowledg*e (pengetahuan seseorang) untuk tiap area dapat dilihat pada tabel 9 berikut ini:

Tabel 9. Total Nilai Kesadaran Keamanan Informasi

Dimensi	Area						Total Nilai
	A1	**A2**	**A3**	**A4**	**A5**	**A6**	
*Knowledg*e	80	74	90	75	88	69	79
Attitude	60	90	85	76	90	76	80
Behaviour	20	86	75	50	60	33	54
Total Nilai	53	83	83	67	61	59	71

Dari tabel 9 diketahui bahwa total nilai kesadaran untuk semua dimensi dari semua area yang ada adalah sebesar 71%. Berdasarkan tabel 6 yang merupakan level kesadaran keamanan informasi menunjukkan bahwa dengan hasil tersebut level kesadaran keamanan informasi mahasiswa STMIK XYZ berada pada level "sedang". Hal ini berarti bahwa kesadaran keamanan informasi mahasiswa STMIK XYZ perlu perhatian khusus untuk diarahkan menuju sikap dan perilaku dengan pengetahuan yang dapat diterima. Untuk menunjang tindakan perbaikan ataupun pembenahan perlu dilakukan kegiatan monitoring secara berkelanjutan. Jika ditinjau dari dimensi-dimensi yang ada, dimensi *Knowledg*e menunjukkan hasil sebesar 79% hal ini menunjukkan bahwa level kesadaran keamanan informasi mahasiswa STMIK XYZ pada dimensi *Knowledg*e berada pada level "sedang" (sudah mendekati baik). Hal ini berarti bahwa pada dimensi ini hasilnya sudah bisa dikatakan baik hanya perlu pembenahan sedikit. Hasil pengukuran pada dimensi *Attitude* menunjukkan hasil sebesar 80% hal ini menunjukkan bahwa level kesadaran keamanan informasi mahasiswa STMIK XYZ pada dimensi *Attitude* sudah baik sehingga perlu dipertahankan. Hasil yang sangat berbeda justru dijumpai pada dimensi *Behaviour* yang menunjukkan hasil sebesar 79% sehingga pada dimensi *Behaviour* dikategorikan berada pada level "buruk". Hal ini berarti bahwa kesadaran keamanan informasi mahasiswa STMIK XYZ pada dimensi *Behaviour* perlu tindakan pembenahan/perbaikan yang bentuknya dapat berupa sosialisasi cara menggunakan internet/social media secara bijak ataupun himbauan-himbauan untuk memberikan kesadaran dalam menjaga keamanan informasi.

Jika ditinjau dari masing-masing area, ada tiga area yang memiliki nilai dibawah 59 yaitu area *policies, mobile equipment dan consequences*. Hal ini menunjukkan bahwa level kesadaran keamanan informasi mahasiswa STMIK XYZ pada area tersebut berada pada level "buruk". Dengan demikian perlu perhatian khusus dari semua pihak terkait terutama pihak lembaga perguruan tinggi. Tindakan-tindakan seperti imbauan/motivasi untuk tetap mengikuti SOP/peraturan yang telah ditetapkan seperti tidak meninggalkan laptop/komputer dalam posisi tidak di-*lock* ataupun sosialisasi/imbauan untuk selalu berhati-hati dalam menggunakan perangkat seluler khususnya di area-area bebas yang rentan terhadap keamanan informasi. Untuk area-area lain yang sudah berada pada level "sedang" dan "baik" perlu dipertahankan dan ditingkatkan ke hasil yang maksimal.

5. KESIMPULAN

Secara umum level kesadaran keamanan informasi mahasiswa STMIK XYZ sudah berada pada level "sedang"dan hampir mendekati baik dengan total nilai keseluruhan 71%. Dengan demikian hanya perlu dipertahankan yang sudah baik dan ditingkatkan yang masih berada pada level sedang. Perlu tindakan monitoring yang berkelanjutan untuk memastikan proses ke arah itu dapat tercapai. Kerjasama dengan semua pihak untuk meningkatkan

kesadaran terhadap keamanan informasi juga perlu dilakukan. Dari tiga dimensi yang ada hanya dimensi *Behaviour* yang memberikan hasil yang "buruk". Begitu juga dengan area pengukuran, dari enam area pengukuran, ada tiga area yang memberikan hasil yang "buruk". Area tersebut adalah "Selalu taat pada aturan perusahaan", "Berhati-hati menggunakan perangkat seluler" dan "Menyadari konsekuensi setiap tindakan". Terlebih lagi dari tiga area yang "buruk" tersebut semuanya berkaitan dengan dimensi *Behaviour*. Dengan demikian dimensi *Behaviour* perlu mendapatkan perhatian khusus dari pihak terkait untuk dilakukan pembenahan supaya hasilnya dapat ditingkatkan. Kegiatan sosialisasi, himbauan maupun pelatihan-pelatihan yang berkaitan dengan kesadaran keamanan informasi dapat dilakukan dalam upaya pembenahan kesadaran keamanan informasi.

DAFTAR PUSTAKA

[1] Mukhlis Amin., 2014, *Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA), Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika*, Vol 5, hal 15-24.

[2] Rio Wirawan, Haris Nizhomul Haq., 2019, *Studi Kompetensi dan Kesadaran Pengguna E-Learning Terhadap Keamanan Sistem E-Learning Pada Pendidikan Tinggi, Jurnal Penelitian dan Pengabdian kepada Masyarakat*, Vol 5, hal 15-24.

[3] Jogiyanto., 2009, *Analisis & Desain*, Andi Offset, Yogyakarta.

[4] McLeod, Raymond & Schell, George P, 2008, *Sistem Informasi Manajemen*, Edisi 10, Salemba Empat, Jakarta.

[5] Witman, M. E., Mattord, H. J., 2011, *Principles of Information security*, 4th Edition, Cengage Learning, Atlanta.

[6] Krugger, H. A., & Kearney, W. D., 2006, *A Prototype for Assesing Information Security Awareness*, Elsevier 25 *Computer & Securitiy* pp. 289-296.

[7] Belton, V., & Stewart, T. J., 2002, *Multiple Criteria Decision Analysis: An Integrated Approach*, Kluwer Academic Publishers.

[8] Sugiyono, 2011, *Metode Penelitian Kuantitatif kualitatif dan R & D*, Alfabeta, Bandung

[9] Sekaran, Uma, 2006, *Metodologi Penelitian untuk Bisnis*, Edisi 4, Buku 2, Salemba Empat, Jakarta.