Jurnal Ilmiah Sinus (JIS) Vol : 20, No. 1, Januari 2022
ISSN (Print) : 1693-1173, ISSN (Online): 2548-4028

Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat *Study From Home* dengan *Multiple Criteria Decision Analysis (MCDA)*

Andriani Kusumaningrum[1)], Hendro Wijayanto[2*)], Bayu Dwi Raharja[3)]
[1,3)] Program Studi Sistem Informasi Akuntansi, STMIK Sinar Nusantara Surakarta
[2)] Program Studi Informatika, STMIK Sinar Nusantara Surakarta
[1)] andriani@sinus.ac.id 1, [2)] hendro@sinus.ac.id, [3)] bayudr@sinus.ac.id

ABSTRACT

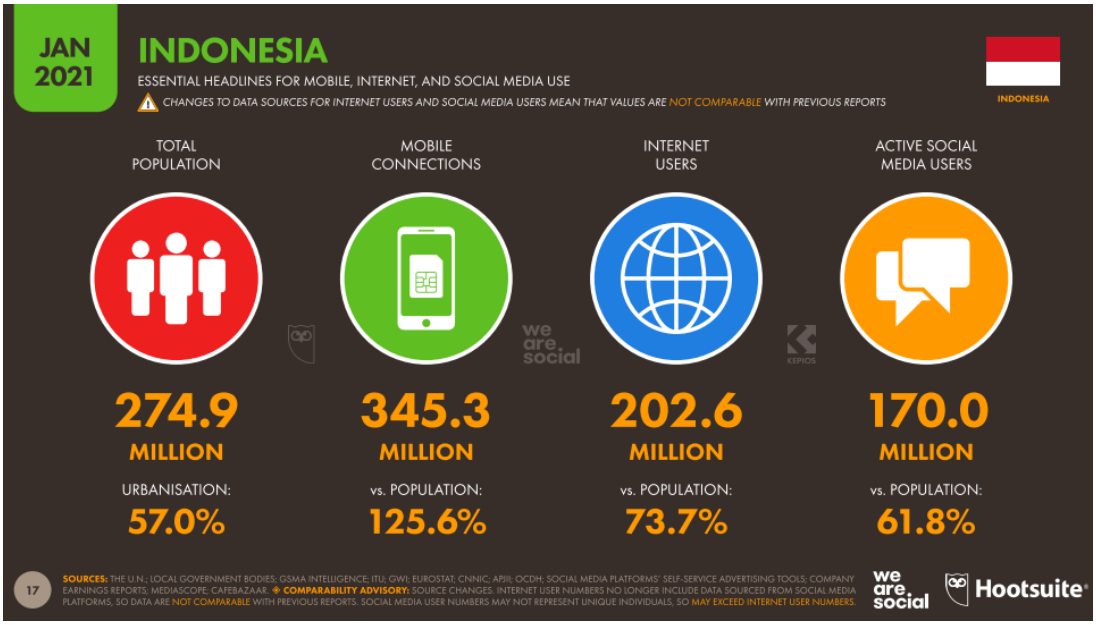
Covid-19 pandemic has forced all sectors to be online. Likewise in higher education, college students must carry out their learning activities from home and use computer information technology. This high digital activity will make cyber-crime high. Measurement of cybersecurity awareness for students when studying from home can be a reference to educate students on the importance of cybersecurity. Its measurement used multiple criteria decision analysis or MCDA. Multi-criteria decision analysis (MCDA) is one of the elements risk managements contained in SNI ISO 31000. The measured dimensions were knowledge, attitude and behavior within areas of using passwords, email and internet, mobile devices, social media, incidents and consequences. The calculation of the weighting used the analytic hierachy process or AHP method. The results of the measurements showed a total value of 79.5% or entered at a moderate level. At this level, students already have good knowledge of cybersecurity readiness. However, students have not been maximal in applying it to their daily activities. The assessment of the knowledge dimension showed a value of 84%, attitude of 78.3% and behavior of 73.1%. It needs to be an increase in socialization in terms of cybersecurity. This result was 8.5% difference from previous research with different object and question components. It still showed the level of awareness at the level of "medium". Therefore, college students are better understanding the importance of cyber security and encourage themselves to become cybersecurity agents in the community.

Keywords *: Cybersecurity, Cybercrime, Cybersecurity Awareness, Multiple Criteria Decision Analysis, Analytic Hierarchy Process*

I. PENDAHULUAN

Pandemi Covid-19 yang sudah masuk tahun kedua membuat banyak sektor mengalami permasalahan. Mulai dari sektor ekonomi, sosial budaya, pendidikan sampai dengan teknologi. Hal positif yang terjadi di masa pandemi ini salah satunya terjadi di sektor teknologi informasi. Dengan adanya *work from home* dan *study frome home*, memaksa penggunaan teknologi informasi di semua bagian. Transformasi digital terjadi dengan sendirinya dan berjalan begitu cepat. Seiring pemaksaan penggunaan teknologi informasi dan komputer selama pandemi.

Berdasarkan rilis dari We Are Social and Hotsuite pada kuartal pertama tahun 2021 yang ditunjukkan pada Gambar 1, bahwa total pertumbuhan penduduk Indonesia sebesar 274,9 Juta jiwa. Sedangkan populasi penggunaan Smartphone sebesar 125,6% dari total penduduk. Untuk pengguna Internet sebesar 73,7%. Dari sisi pengunaan sosial media, urutan pertama ditempati oleh Whatsapp, kemudian Facebook dan Instagram. Selain media sosial, penggunaan aplikasi selama pandemi juga sangat tinggi. Penggunaan aplikasi belanja sebesar 78,2%, finansial dan perbankan 39,2%, dan kesehatan 23,4% (Social, 2021). Kondisi ini mengalami peningkatan di tahun sebelumnya, yang mana perjalanan pandemi baru memasuki tahun pertama. Jika dilihat dari persentase diatas, dapat dilihat bahwa terjadi peningkatan penggunaan teknologi informasi dan komputer.



Gambar 1. Sebaran Populasi dan penggunaan smartphone, internet serta media sosial

Tanpa disadari dengan tingginya penggunaan teknologi informasi ini, akan semakin tinggi pula tingkat kejahatan siber yang akan terjadi. Mulai dari serangan hoax, penipuan, pencurian dan penyalahgunaan data. Dari data yang dihimpun oleh Interpol selama 4 bulan antara Januari sampai April 2020, terjadi 907.000 *spam*, 737 insiden *malware*, 48.000 *malicious URLs* (Interpol, 2020). Serangan siber yang sangat sering selain laporan dari Interpol adalah kejahatan yang menargetkan sistem kesehatan, pengambilan keuntungan perusahaan, mata-mata dan kejahatan yang digunakan untuk tujuan keuntungan, dan pemanfaatan kesalahan/ketidaktahuan manusia terhadap kejadian pandemi Covid-19 dalam hal informasi, berita, maupun penggunaan aplikasi Covid-19 (Mahadevan, 2020). Dari kejadian ini, dunia pendidikan juga tak luput dari kejadian serangan siber. Karena seluruh kegiatan pendidikan dilakukan secara daring. Baik menggunakan aplikasi pendidikan maupun aplikasi sosial media konvensional. Dari penelitian yang sudah dilakukan di tingkat pendidikan tinggi secara umum pada pertengahan tahun 2020 menunjukkan tingkat kesiapan keamanan siber yang sangat rendah. Dari sisi teknologi dan keamanan menunjukkan skala 4.36 (Cukup), sedangkan dari sisi kontrol dan kerusakan serangan siber menunjukkan skala 1,31 (Tidak Siap) (Hendro & Iwan Ady, 2020).

Tingkat kerentanan ini akan mungkin terminimalisir jika berada di dalam sistem yang mengedepankan kesiapan serangan siber (*cybersecurity readiness*) yang baik. Akan tetapi berbeda dengan pelaku di tingkat perguruan tinggi yang lainnya. Khususnya mahasiswa yang melakukan *study from home*. Tingkat literasi digital yang belum terlalu cukup dan tidak adanya pengawasan dari perguruan tinggi, membuat tingginya serangan siber menimpa kalangan mahasiswa. Perlu adanya pengukuran tingkat kesiapan keamanan siber di sisi mahasiswa, sehingga diperoleh nilai untuk dapat diambil kebijakan dan sosialisasi akan pentingnya keamanan siber.

Analisis keputusan multikriteria atau *Multi Criteria Decision Analysis (MCDA)* merupakan salah satu elemen manajemen resiko yang terkandung dalam SNI ISO 31000. Terdiri dari tiga rangkaian kegiatan, yaitu identifikasi resiko, analisis resiko, dan evaluasi resiko (Salvatore, Matthias, & Jose Rui, 2016). Model inilah yang nantinya digunakan untuk mengidentifikasi kebiasaan mahasiswa yang akan menimbulkan celah keamanan siber, mengidentifikasi bagian-bagian keamanan dan melakukan evaluasi terhadap kebiasaan-kebiasaan mahasiswa. Dari beberapa penelitian terkait dengan penggunaan analisis

keputusan multikriteria ini juga pernah dilakukan oleh (David & Dorie, 2020) yang melakukan analisis terhadap kesiapan keamanan informasi dengan konsep pengukuran yang sederhana. Analisis yang dilakukan hanya berpusat pada suatu perguruan tinggi dan pada program studi tertentu saja. Sehingga kompleksitas responden masih sangat kurang.

II. TINJAUAN PUSTAKA

2.1 Kejahatan Siber

Dari sisi bahasa, siber memiliki arti dunia maya. Sehingga kejahatan siber merupakan praktik untuk merusak, mencuri, menyalahgunakan sistem, jaringan, program data dan informasi yang terbuka dan tersambung di dunia maya. Motif kejahatan siber saat ini sangat banyak. Mulai dari kejahatan yang dilator belakangi oleh iseng semata sampai mencari keuntungan profit. Ada beberapa konsep keamanan siber yang dipaparkan oleh (Chan, 2011) yang antara lain :

1. *Phising*. Usaha untuk mendapatkan informasi rahasia atau melakukan pencurian identitas dengan menggunakan e-mail, website palsu yang meniru alamat aslinya. Phising biasanya dilakukan bersamaan dengan cara seperti Social Engineering atau Spaming. Phising merupakan ancaman umum yang dapat terjadi oleh siapapun jika literasi keamanan siber kurang.
2. *Spam*. Surat atau pesan elektronik komersial yang tidak diinginkan oleh penerimanya. Spam ini menjadi bagian dari kejahatan siber terbesar selama pandemi Covid-19. Mulai dari tawaran asuransi kesehatan, informasi Covid-19, tawaran organisasi kesehatan lainnya. Kebanyakan *spam* berisi phising yang sangat berbahaya bagi pengguna yang membukanya.
3. *Social Engineering*. Dalam konteks keamanan informasi, Social Engineering adalah penggunaan sarana non-teknis untuk melakukan pencurian identitas atau informasi rahasia dengan cara kombinasi manipulasi psikologi korbannya. Mitigasi *Social Engineering* sangat tergantung pada kesadaran penggunanya tentang konsep dan penegakan kebijakan yang berkaitan dengan keamanan dan privasi.
4. *Strong Password*. *Password* adalah kunci untuk otentikasi pengguna dan untuk mencegah akses yang tidak sah. Banyak sekali pengguna teknologi informasi menggunakan *password* yang kurang kuat. Atau menggunakan *password* yang merupakan informasi pribadi, misalkan tanggal lahir, nama lengkap, atau identitas pribadi lainnya. Sehingga sangat mudah untuk ditebak maupun diakses dengan model *Brute Force*.
5. *Data or Information Integrity*. Integritas data dan informasi memiliki ciri akurasi, kepercayaan, keberlakuan dan ketepatan waktu. Akurasi dan kebenaran yaitu informasi harus kuat dan benar dalam artian data harus tepat dan sesuai dengan kenyataan. Kepercayaan memastikan akurasi dan kebenaran sehingga seseorang dapat mempercayai informasi tersebut. Keberlakuan dan ketepatan waktu adalah penggunaan informasi harus sesuai dengan kejadian dan waktunya. Sehingga informasi keberlakuan dipengaruhi oleh perubahan kenyataan dari waktu ke waktu dan harus dipenuhi.
6. *Social Networking*. Banyak sekali sosial media yang memberikan pelayanan ekstra terhadap kenyamanan penggunanya. Tetapi dilain sisi, penyedia sosial media dapat mengambil seluruh data dan informasi pengguna. 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 Siber

Tingginya penggunaan teknologi informasi dan komputer yang begitu tinggi, membuat masyarakat harus mulai sadar akan bahayanya kejahatan siber. Kesadaran akan keamanan siber perlu dibangun untuk meminimalisir terjadinya serangan siber. Beberapa penelitian menujukkan hasil kesadaran di tingkat rata-rata. Dalam hasil analisis kesadaran keamanan di kalangan pengguna *E-wallet* di Indonesia menunjukkan nilai 91 dari nilai maksimal 100, atau masuk di kategori rata-rata. Yang mana masih terbuka peluang terjadinya serangan siber (Muhammad Sulthon & Ahmad R, 2021).

Dari sisi pendidikan tinggi juga telah dilakukan analisis terkait dengan perilaku keamanan siber dengan objek penelitian perguruan tinggi wilayah Jawa Tengah. Model pengukuran menggunakan *Cybersecurity Vulnerability Behavior Scale* dengan nilai rata-rata 3,3 dari nilai total 5 untuk kategori kerentanan serangan siber. Atau dapat disimpulkan masuk ke kategori rentan. Adapun variabel yang digunakan meliputi penggunaan *password*, akses data dan informasi, penggunaan perangkat internet, penggunaan sosial media dan penggunaan smartphone (Hendro & Iwan Ady, 2020). Pengukuran kesadaran keamanan siber juga dapat dilakukan dalam organisasi yang cukup besar. Seperti dalam instansi pemerintahan yang dilakukan oleh (Mukhlis, 2014) dalam mengukur tingkat kesadaran keamanan informasi pegawai negeri sipil di Kota Makasar dengan hasil nilai 75% dari total 100% memiliki tingkat kesadaran sedang.

Kesadaran kejahatan siber ditingkat kesehatan, khususnya pengguna teknologi informasi juga telah dilakukan analisis dengan memodelkan berdasarkan *Risky Security Behavior Scale (RScB)* dan *Human Aspect of Information Security Questionaire (HAIS-Q)*. Hasil dari kombinasi tersebut berupa kerangka kesiapan serangan siber di sektor kesehatan dengan variabel penggunaan perangkat komputer, akses sistem informasi kesehatan, perilaku berinternet dan cara menghadapi kejadian tidak wajar teknologi informasi (Penggalih Mahardika, Sylvia, Hendro, & Murni, 2020).

Menurut McLeod dan Schell, Keamanan informasi ditunjukkan untuk mencapai tiga tujuan utama yaitu kerahasiaan, ketersediaan dan integritas (Raymond & George P, 2008). Menurut Kruger dan Kerney (Krugger & Kearney, 2006), menggunakan teori psikologi sosial membagi menjadi tiga komponen, yaitu *cognition*, *affection* dan *behaviour*. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal dengan *Knowledge* (pengetahuan seseorang), *Attitude* (sikap seseorang), dan *Behavior* (perilaku seseorang). 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

2.3 Multiple Criteria Decision Analysis (MCDA)

Salah satu elemen proses manajemen resiko yang terkandung dalam SNI ISO 31000 adalah asesmen resiko. Elemen ini terdiri dari tiga rangkaian kegiatan, yaitu identifikasi resiko, analisis resiko, dan evaluasi resiko. Ketiga kegiatan tersebut dilakukan untuk menilai seberapa penting resiko tersebut bagi organisasi/institusi, serta sebagai landasan sebelum melakukan perilaku resiko. Teknik asesmen resiko dapat dilakukan dengan berbagai alat bantu, salah satunya adalah menggunakan Analisis Keputusan Multikriteria atau *Multiple Criteria Decision Analysis (MCDA)* (Antonius, 2019). Alat bantu ini cocok digunakan untuk seluruh kegiatan asesmen resiko, terutama dalam menilai konsekuensi dan tingkat resiko

 DOI : https://doi.org/10.30646/sinus.v20i1.586

pada kegiatan analisis resiko. Proses analisis keputusan multikriteria dapat dilakukan dengan lima langkah, yaitu menentukan sasaran, menentukan kriteria, melakukan pembobotan kriteria, membuat penilaian dan menentukan rekomendasi keputusan. Metode Multiple Criteria Decision Analysis (MCDA) biasanya digunakan untuk mengambil keputusan atas beberapa alternative yang memiliki banyak kriteria. Metode Multiple Criteria Decision Analysis digunakan untuk mengukur nilai total alternative berdasarkan kriteria-kriteria tertentu. Pendekatan MCDA dibedakan menjadi tiga kategori (Mahdi & Ferenc, 2011) yaitu :

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

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

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

Dimana *V(a)* adalah nilai seluruh alternative *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*.

III. METODE PENELITIAN

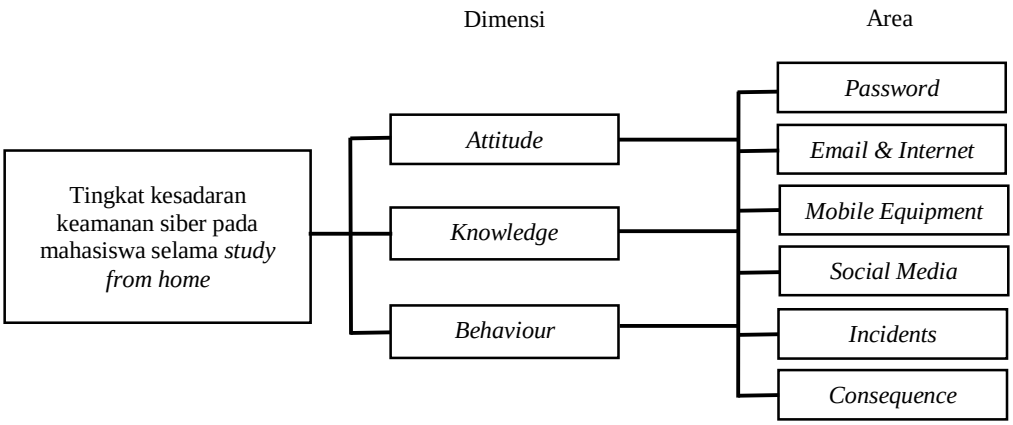
Penelitian ini dilakukan melalui beberapa tahapan dengan menggunakan metode-metode tertentu. Adapun tahapan penelitian adalah sebagai berikut :

3.1. Studi Literatur

Studi literatur digunakan untuk melihat kebiasaan mahasiswa selama *study from home*, menentukan variabel kriteria tingkat keamanan siber untuk dipetakan ke konsep pengukuran tingkat kesadaran keamanan siber. Studi literature ini menggabungkan beberapa model yaitu *Risky Security Behavior Scale (RScB), Human Aspect of Information Security Questionaire (HAIS-Q)* dan melakukan observasi karakteristik kebiasaan dari mahasiswa dalam penggunaan teknologi informasi computer selama *study from home*. Dari hasil studi literatur diperoleh area yang dapat digunakan dalam konsep pengukuran kesadaran keamanan siber di kalangan mahasiswa, yang berisi kesadaran tentang penggunaan *password*, *email* dan internet, perangkat *mobile*, sosial media, kejadian, serta konsekuensi.

3.2. Metode Pengambilan Data

Pengumpulan data dilakukan selama masa pandemi Covid-19 dan pada masa *study from home* untuk mahasiswa. Pengumpulan data menggunakan metode kuesioner dengan populasi adalah mahasiswa dari berbagai program studi di perguruan tinggi Propinsi Jawa Tengah. Adapun yang mengisi kuesioner sebanyak 181 responden. Sedangkan konsep pertanyaan yang diajukan mengacu pada kerangka pengukuran kesadaran keamanan siber yang diperkenalkan oleh Krugger & Kerney. Tingkat kesadaran keamanan siber mahasiswa ini diukur berdasarkan dimensi *knowledge* (pengetahuan), *attitude* (sikap), dan *behaviour* (perilaku). Adapun area yang digunakan dalam konsep pengukuran dengan ketiga dimensi tersebut adalah *password*, *email* & internet, *mobile equipment*, social media, *incidents*, dan *consequences*. Konsep pengukuran dapat dilihat pada Gambar 2.



Gambar 2. Konsep Pengukuran Kesiapan Keamanan Siber Pada Mahasiswa saat *study from home*

Untuk menguji *knowledge* (pengetahuan), *attitude* (sikap) dan *behaviour* (perilaku) responden berkaitan dengan enam area kesadaran keamanan siber disusunlah pentanyaan sebanyak 18 (delapan belas) buah, atau masing-masing area memiliki 3 (tiga) pertanyaan. Setiap pertanyaan diberikan jawaban dengan 3 skala yaitu, benar, salah, dan tidak tahu. Pertanyaan ini digunakan untuk menghitung nilai $v_i(a)$. Adapun contoh pertanyaan area kesadaran keamanan siber pada mahasiswa selama *study from home* dapat dilihat pada tabel 1.

Tabel 1 Contoh pertanyaan pada masing-masing dimensi

No	Dimensi *Knowledge*	Dimensi *Attitude*	Dimensi *Behaviour*
1	*Password* merupakan salah satu cara untuk melindungi suatu akses ilegal ke perangkan maupun akun *(password area)*	Perangkat mobile, akun, sosial media dan lainnya perlu diproteksi dengan memanfaatkan *password (password area)*	Mahasiswa sadar bahwa seharusnya tidak memberikan *password* kepada orang lain. *(password area)*
2	Didalam email terdapat data-data dan informasi rahasia dari pemiliknya. Penggunaan internet gratis (*free hotspot*), menjadi salah satu ancaman kebocoran data. *(email & internet area)*	Akun email merupakan hal yang perlu dilindungi dari akses pihak ketiga. Penggunaan perangkat internet mandiri dapat meminimalisir terjadinya kebocoran data. *(email & internet area)*	Mahasiswa sadar bahwa memberikan akun email ke orang lain akan menyebabkan bocornya data pribadi. *(email & internet area)*
3	Dengan kecerobohan mengumbar data pribadi dalam perangkat mobile dan sosial media, akan menjadikan target kejahatan siber. *(incident area)*	Memproteksi perangkat mobile, sosial media serta tidak mengumbar data pribadi akan meminimalisir terjadinya kejahatan siber. *(incident area)*	Mahasiswa sadar bahwa perangkat mobile dan sosial media merupakan cerminan pribadi yang berisi data dan informasi pribadi, serta harus dilindungi. *(incident area)*

Langkah selanjutnya setelah memperoleh nilai $v_i(a)$ adalah dengan melakukan penghitungan perkalian dengan bobot w_i. Bobot w_i ditentukan dengan menggunakan metode *analytic hierarchy process* atau *AHP*, dimana metode ini menjadi salah satu metode dari *Multiple Criteria Decision Analysis (MCDA)*. Kemudian dalam menentukan bobot pada masing-masing dimensi berdasarkan skala yang digunakan oleh Krugger & Kerney yang dapat dilihat pada Tabel 2.

Tabel 2. Bobot Masing-masing Dimensi

Dimensi	Bobot
Knowledge	30
Atittude	20
Behaviour	50

Sebelum ditentukan tingkat kesadaran keamanan siber sebagai hasil akhir, untuk proses perhitungan total skor untuk tiap dimensi dan tiap area dapat dilihat pada Tabel 3.

Tabel 3. Perhitungan Total Nilai

Dimensi	**Area**						**Total Nilai**
	A1	**A2**	**A3**	**A4**	**A5**	**A6**	
Knowledge	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	$\sum_{i=1}^{3} Ai1/3$	$\sum_{i=1}^{3} Ai2/3$	$\sum_{i=1}^{3} Ai3/3$	$\sum_{i=1}^{3} Ai4/3$	$\sum_{i=1}^{3} Ai5/3$	$\sum_{i=1}^{3} Ai6/3$	

Kemudian selanjutnya menentukan level kesadaran keamanan siber pada mahasiswa selama *study from home*. Level yang ditetapkan yaitu baik, sedang dan buruk. Masing-masing level memiliki *range* nilai yang dapat ditunjukkan pada Tabel 4.

Tabel 4. Level Tingkat Kesadaran Keamanan Siber

Hasil Pengukuran (dalan persen)	**Level**	**Keterangan**
80 – 100	Baik	Pada level ini mahasiswa mampu dan siap dalam hal kesadaran keamanan siber baik dari sisi pengetahuan, sikap dan perilaku.
60 – 79	Sedang	Pada level ini mahasiswa cukup dalam hal kesadaran keamanan siber baik dari sisi pengetahuan, sikap dan perilaku. Perlu adanya peningkatan kesadaran keamanan siber untuk meminimalisir kejadian serangan siber yang lebih berbahaya.
0 – 59	Buruk	Pada level ini mahasiswa **harus** meningkatkan kesadaran keamanan siber baik dari sisi pengetahuan, sikap dan perilaku. Di level ini akan sangat berbahaya jika mahasiswa mengalami serangan siber. Karena belum cukup memahami bagaimana langkah terdekat dalam menangani kejadian siber. Pengayaan literatur baik dari bacaan maupun pakar sangat diperlukan.

IV. HASIL DAN PEMBAHASAN

Berdasarkan hasil kuesioner, terdapat 181 responden yang melakukan pengisian. Dari 181 responden ini terdapat 14 responden yang dihilangkan karena proses normalisasi hasil kuesioner. Sehingga data yang digunakan sebanyak 167 responden. Adapun untuk sebaran wilayah yang melakukan pengisian kuesioner dapat dilihat pada tabel 5 berikut :

Tabel 5. Sebaran Responden Berdasarkan Kota/Kabupaten

Kota/Kabupaten	**Jumlah Responden**
Surakarta	82
Semarang	44
Pati	11
Salatiga	13
Purwokerto	8
Kudus	9

Untuk hasil perhitungan pembobotan pada setiap area dengan menggunakan metode *analytic hierarchy process (AHP)* dapat dilihat pada Tabel 6.

Tabel 6. Hasil Pembobotan dengan AHP

Area	Hasil w_i
Password	0.7
Email & Internet	0.5
Mobile Devices	0.6
Social Media	0.4
Incidents	0.3
Consequence	0.2

Dari tabel 6 diperoleh hasil bahwa nilai paling tinggi berada pada area *password*, kemudian disusul *mobile devices*. Hal ini menunjukkan bahwa mahasiswa selama *study from home* sadar bahwa penggunaan *password* baik dengan kombinasi angka huruf, *Personal Identity Number* (*PIN)* maupun *One Time Password (OTP)*, sangat penting dalam melindungi data dan informasi. Mahasiswa juga menyadari dan mengetahui bahwa perangkat *smartphone* yang mereka gunakan merupakan perangkan yang perlu dilindungi. Karena didalamnya tersimpan banyak sekali informasi dan data penting. Terutama data pribadi pemilik *smartphone*.

Dengan menggunakan rumus (1) maka hasil penghitungan level kesadaran keamanan siber untuk masing-masing dimensi dan tiap area dapat dilihat pada Tabel 7.

Tabel 7. Total Nilai Kesadaran Keamanan Siber

Dimensi	Area						Total Nilai
	A1	A2	A3	A4	A5	A6	
Knowledge	88	74	90	85	88	79	84
Attitude	72	80	85	76	80	77	78.3
Behaviour	78	86	85	50	70	70	73.1
Total Nilai	79	80	87	70	82	79	**79.5**

Dari tabel 7 diketahui bahwa total nilai kesadaran untuk semua dimensi dari semua area sebesar 79,5%. Jika dilihat berdasarkan tabel 4 atau tabel level kesadaran keamanan siber, menunjukkan bahwa hasil tersebut masuk di level "**sedang**" dan hampir mendekati "**baik**". Dimana pada level ini mahasiswa perlu meningkatkan kembali kesadaran keamanan siber. Jika dilihat dari dimensinya, pengetahuan mahasiswa dibidang keamanan siber memang sudah baik. Hanya perlu adanya peningkatan dibidang perilaku dan sikap. Banyak dari mahasiswa sudah menyadari akan pentingnya keamanan siber, tetapi terkadang menganggap remeh beberapa aturan-aturan yang dapat membuat data informasi disalahgunakan. Semisal contohnya adalah penggunaan *password/PIN/OTP*. Mahasiswa menyadari bahwa penggunaan *password/PIN/OTP* sangat penting dalam melindungi data informasi dan akun. Tetapi terkadang mahasiswa membuat password dengan password yang mudah ditebak.

Pada penelitian terdahulu (David & Dorie, 2020) dengan jumlah responden 252 mahasiswa program studi dibidang teknologi informasi dan komputer pada STMIK XYZ menunjukkan hasil dari kesiapan keamanan informasi sebesar 71% atau masuk di level "**sedang**". Hasil ini selisih 8,5% dari penelitian yang dilakukan dengan objek yang berbeda dan komponen pertanyaan yang berbeda. Tetapi untuk level yang diperoleh masih menunjukkan pada level "**sedang**". Hal ini dapat disimpulkan bahwa kesadaran keamanan siber tidak hanya diperlukan bagi mahasiswa yang berpendidikan bukan komputer saja, tetapi juga bagi mahasiswa yang berpendidikan di bidang teknologi informasi dan komputer.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Secara umum level kesadaran mahasiswa dalam hal keamanan siber khususnya pada saat pandemi Covid-19 atau saat *study from home* sudah berada pada level "**sedang**" dengan total nilai keseluruhan 79,5%. Angka ini mendekati level baik. Hasil ini selisih 8,5% dari penelitian yang dilakukan sebelumnya dengan objek yang berbeda dan komponen pertanyaan yang berbeda. Tetapi untuk level yang diperoleh masih menunjukkan pada level "**sedang**". Mahasiswa perlu membiasakan diri dan konsisten dalam meningkatkan perilaku keamanan siber. Secara pengetahuan/*knowledge* mahasiswa sudah baik dalam memahami pentingnya keamanan siber. Sehingga tinggal membiasakan diri terhadap aturan-aturan keamanan siber. Hal ini sangat penting mengingat pandemi Covid-19 ini memaksa mahasiswa menggunakan teknologi informasi dan komputer secara penuh dalam studinya. Semakin sering bersentuhan dengan teknologi, peluang kejahatan siber juga semakin tinggi.

5.2 Saran

Perlu adanya peningkatan sosialisasi dalam hal keamanan siber. Sehingga mahasiswa lebih memahami dan mengerti pentingnya keamanan siber, serta mendorong mahasiswa menjadi agen keamanan siber dilingkungan masyarakat.

Penelitian kedepan dapat dilakukan pada cakupan yang lebih luas dengan responden yang banyak. Objek penelitian juga tidak terbatas pada mahasiswa, tetapi dapat lebih luas seperti tenaga kependidikan maupun tenaga pengajar.

DAFTAR PUSTAKA

Social, W. A. (2021). *Digital 2021*. United State: We Are Social and Hot Suite Report.

Interpol. (2020, August 4). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Retrieved from Interpol: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Mahadevan, P. (2020). *Cybercrime. Threats during the COVID-19 pandemic*. Switzerland: Global Initiative Against Transnational Organized Crime.

Hendro, W., & Iwan Ady, P. (2020). *Kesiapan Perguruan Tinggi Wilayah Jawa Tengah Dalam Menghadapi Serangan Siber: Policy Brief*. Semarang: Lembaga Penelitian dan Pengabdian pada Masyarakat Universitas Dian Nuswantoro.

Salvatore, G., Matthias, E., & Jose Rui, F. (2016). *Multiple Criteria Decision Analysis. States of the Art Survey*. New York: Springer.

Chan, H. (2011). *Information Security Awarness of TAFE South Australia Employees*. Australia: Computer and Information Science Universuty of South Australia.

Muhammad Sulthon, A., & Ahmad R, P. (2021). Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia. *Automata*, *2*(1).

Hendro, W., & Iwan Ady, P. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal SISFOKOM (Sistem Informasi dan Komputer)*, *9*(3), 395-399.

Mukhlis, A. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika, 5*(1), 15-24.

Penggalih Mahardika, H., Sylvia, A., Hendro, W., & Murni. (2020). Model Perilaku Keamanan Siber Pada Pengguna Sistem Informasi Kesehatan Pada Masa Pandemi Covid-19 Cyber Security Behavior Model on Health Information System Users During Covid-19 Pandemic. *Cyber Security dan Forensik Digital*, *3*(2), 28-33.

Antonius, A. (2019). *Multi-criteria Decision Analysis.* Bandung: CyberWhale.

Mahdi, Z., & Ferenc, S. (2011). *Multicriteria Analysis. Applications to Water and Environment Management.* New York: Springer.

Raymond, M., & George P, S. (2008). *Sistem Informasi Manajemen. Edisi 10.* Jakarta: Salemba Empat.

Krugger, H., & Kearney, W. (2006). A Prototype for Assesing Information Security. *Computer & Security*, 289-296.

David, & Dorie. (2020). Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa. *Jurnal Teknik Informatika dan Sistem Informasi, 7*(1), 11-20.