Jurnal Vocational Teknik Elektronika dan Informatika
http://ejournal.unp.ac.id/index.php/voteknika
Universitas Negeri Padang, Indonesia

ISSN 2302-3295 (Print)
ISSN 2716-3989 (Electronics)
Vol. 14, No. 1, 2026

The Effects of Perceived Threat and Perceived Vulnerability on Security Awareness Through Cybersecurity Engagement

Erliza Yubarda[1*], M Giatman[2], Hasan Maksum[2], Remon Lapisa[2], Nurindah Dwiyani[2]

[1] Universitas Negeri Padang, Padang, Indonesia

[2] Sekolah Tinggi Ilmu Pelayaran (STIP), Jakarta, Indonesia

*Corresponding Author: hadiksaputra@ft.unp.ac.id

Abstract - **Digital transformation has intensified students' dependence on information technology while simultaneously increasing their exposure to cybersecurity risks. Consequently, enhancing security awareness has become essential for safeguarding personal and institutional digital assets. This study investigates the effects of perceived threat and perceived vulnerability on security awareness through the mediating role of cybersecurity engagement. Grounded in Protection Motivation Theory (PMT), a quantitative explanatory survey was conducted involving 134 undergraduate students aged 18–24 years at Universitas Negeri Padang, Indonesia. Data were collected through an online questionnaire and analyzed using Partial Least Squares–Structural Equation Modeling (PLS-SEM). The measurement model demonstrated satisfactory reliability and validity, with all constructs meeting the recommended thresholds for convergent validity, discriminant validity, and internal consistency. The structural model revealed that perceived threat ($\beta = 0.434$, $p < 0.001$) and perceived vulnerability ($\beta = 0.359$, $p < 0.001$) significantly enhance cybersecurity engagement, which in turn exerts a strong positive effect on security awareness ($\beta = 0.764$, $p < 0.001$). Furthermore, cybersecurity engagement significantly mediates the effects of perceived threat and perceived vulnerability on security awareness. These findings highlight that security awareness develops not only through risk perception but also through active participation in cybersecurity-related activities. The study contributes to cybersecurity education research and provides practical guidance for designing engagement-oriented cybersecurity awareness programs in higher education institutions.**

Keywords— **Security Awareness, Perceived Threat, Perceived Vulnerability, Cybersecurity Engagement, Protection Motivation Theory**

I. PENDAHULUAN

Transformasi digital yang semakin masif dalam kehidupan masyarakat modern telah membawa perubahan signifikan dalam cara individu belajar, berkomunikasi, dan berinteraksi [1]. Bagi mahasiswa, teknologi digital tidak lagi sekadar alat pendukung akademik, melainkan telah menjadi bagian integral dari kehidupan sehari-hari, baik dalam konteks pembelajaran daring, media sosial, transaksi digital, maupun pengelolaan data pribadi [2]. Namun, di balik manfaat besar tersebut, perkembangan teknologi digital juga diiringi dengan meningkatnya kompleksitas dan intensitas ancaman keamanan siber yang berpotensi merugikan individu secara personal maupun institusional [3].

Berbagai penelitian dan kajian akademik menunjukkan bahwa kelompok usia muda, khususnya mahasiswa, merupakan salah satu kelompok yang paling rentan terhadap kejahatan siber seperti phishing, pencurian identitas, peretasan akun, dan penyalahgunaan data pribadi [4], [5], [6]. Kerentanan ini tidak semata-mata disebabkan oleh keterbatasan teknologi pengamanan, tetapi juga oleh faktor kognitif, psikologis, dan perilaku pengguna itu sendiri. Dalam konteks ini, *security awareness* atau kesadaran keamanan siber menjadi elemen kunci yang menentukan sejauh mana individu mampu mengenali risiko, memahami ancaman, serta menyadari perannya dalam menjaga keamanan digital [7].

Security awareness dipahami sebagai tingkat pengetahuan, kewaspadaan, dan pemahaman individu terhadap risiko dan ancaman keamanan informasi, serta kesadaran akan pentingnya perilaku aman dalam penggunaan teknologi digital. Sejumlah penelitian menegaskan bahwa rendahnya *security awareness* merupakan salah satu penyebab utama kegagalan sistem keamanan informasi, bahkan ketika teknologi pengamanan yang digunakan telah memadai. Dengan kata lain, manusia sering kali menjadi *weakest link* dalam rantai keamanan siber [8].

Pembentukan *security awareness* tidak terjadi secara spontan, melainkan dipengaruhi oleh proses kognitif dan psikologis yang kompleks. Salah satu kerangka teori yang paling banyak digunakan untuk menjelaskan proses ini adalah *Protection Motivation Theory* (PMT). PMT menjelaskan bahwa motivasi individu untuk melakukan perilaku protektif termasuk kesadaran dan kewaspadaan terhadap keamanan siber dipengaruhi oleh dua proses utama, yaitu *threat appraisal* dan *coping appraisal*. Pada tahap *threat appraisal*, individu

DOI: 10.24036/voteteknika.v14i1.137124
Received : 2025-12-25
Revised : 2026-01-04
Accepted : 2026-01-04
Published : 2026-03-31

For all articles published in VOTETEKNIKA https://ejournal.unp.ac.id/index.php/voteknika, © copyright is retained by the authors. This is an open-access article under the CC BY-SA license.

mengevaluasi tingkat ancaman yang dihadapi serta sejauh mana dirinya rentan terhadap ancaman tersebut [9].

Dua konstruk utama dalam *threat appraisal* adalah persepsi ancaman (*perceived threat*) dan kerentanan yang dirasakan (*perceived vulnerability*). Persepsi ancaman merujuk pada sejauh mana individu memandang kejahatan siber sebagai sesuatu yang serius, nyata, dan berpotensi menimbulkan dampak negatif. Sementara itu, *perceived vulnerability* mengacu pada keyakinan individu bahwa dirinya secara personal berisiko menjadi korban serangan siber. Penelitian berbasis PMT menunjukkan bahwa individu yang memiliki persepsi ancaman dan kerentanan yang tinggi cenderung menunjukkan tingkat perhatian dan kewaspadaan yang lebih besar terhadap isu keamanan [10].

Dalam konteks mahasiswa, persepsi ancaman tidak hanya berkaitan dengan keberadaan *hacker* atau penipu online, tetapi juga dengan kesadaran bahwa kelalaian pribadi seperti penggunaan kata sandi yang lemah atau kebiasaan membagikan informasi pribadi secara berlebihan dapat memicu terjadinya pelanggaran keamanan. Penelitian ini secara eksplisit menangkap dimensi tersebut melalui indikator-indikator yang menekankan intensitas ancaman, sumber ancaman, serta tingkat keseriusan ancaman keamanan siber. Hal ini menunjukkan bahwa persepsi ancaman tidak bersifat abstrak, melainkan berakar pada pengalaman dan pemahaman nyata mahasiswa terhadap risiko digital [11].

Persepsi ancaman saja tidak cukup untuk membentuk *security awareness* yang kuat. Sejumlah studi mengemukakan bahwa meskipun individu menyadari adanya ancaman, mereka belum tentu merasa dirinya secara personal rentan terhadap ancaman tersebut. Inilah yang menjadikan *perceived vulnerability* sebagai variabel penting dalam menjelaskan variasi tingkat kesadaran keamanan. Individu yang merasa bahwa akun digitalnya berpotensi diserang, data pribadinya belum aman, atau pertahanan keamanannya memiliki celah, cenderung menunjukkan tingkat kewaspadaan yang lebih tinggi dibandingkan individu yang merasa aman-aman saja [12].

Perceived vulnerability berfungsi sebagai mekanisme internalisasi ancaman, yaitu proses ketika ancaman eksternal dipersepsikan sebagai risiko personal. Dalam literatur PMT, proses ini sangat krusial karena tanpa adanya rasa kerentanan personal, individu cenderung meremehkan risiko dan mengabaikan isu keamanan. *Perceived vulnerability* memiliki pengaruh signifikan terhadap niat dan kesadaran individu dalam menerapkan praktik keamanan informasi [13].

Hubungan antara persepsi ancaman, *perceived vulnerability*, dan *security awareness* tidak selalu bersifat langsung [14]. Sejumlah kajian kontemporer menunjukkan adanya variabel antara yang menjembatani proses kognitif tersebut, salah satunya adalah *cybersecurity engagement* [15], [16]. *Cybersecurity engagement* merujuk pada tingkat keterlibatan aktif individu dalam aktivitas yang berkaitan dengan keamanan siber, seperti mencari informasi keamanan, memperbarui kata sandi, mengikuti pelatihan, berdiskusi dengan orang lain, serta mengambil inisiatif untuk meningkatkan keamanan perangkat dan akun [17].

Cybersecurity engagement menempati posisi yang unik dalam model ini karena ia merepresentasikan transisi dari kesadaran kognitif menuju keterlibatan praktis. Dalam perspektif PMT, *engagement* dapat dipandang sebagai respons awal terhadap appraisal ancaman sebelum terbentuknya kesadaran yang lebih matang dan terinternalisasi. Penelitian keamanan informasi menunjukkan bahwa individu yang terlibat aktif dalam aktivitas keamanan cenderung memiliki tingkat *security awareness* yang lebih tinggi dan lebih stabil [18].

Dalam konteks mahasiswa, *cybersecurity engagement* menjadi sangat relevan karena kelompok ini memiliki akses luas terhadap sumber informasi digital, namun tingkat keterlibatan mereka dalam aktivitas keamanan sering kali bersifat sporadis dan tidak sistematis. Penelitian ini menunjukkan bahwa *engagement* diukur melalui berbagai bentuk keterlibatan aktif, mulai dari pencarian informasi hingga partisipasi dalam kegiatan edukatif. Pendekatan ini memungkinkan pemahaman yang lebih komprehensif tentang bagaimana *engagement* berfungsi sebagai mekanisme mediasi antara appraisal ancaman dan *security awareness* [6].

Dengan demikian, dapat dikatakan bahwa persepsi ancaman dan *perceived vulnerability* mendorong individu untuk lebih terlibat dalam aktivitas keamanan siber. Keterlibatan tersebut, pada gilirannya, memperkuat pemahaman, kewaspadaan, dan rasa tanggung jawab individu terhadap keamanan digital. Proses inilah yang pada akhirnya membentuk *security awareness* yang lebih utuh dan berkelanjutan. Model ini menegaskan bahwa *security awareness* bukan sekadar hasil dari pengetahuan atau pengalaman semata, melainkan merupakan produk dari interaksi dinamis antara persepsi risiko, rasa kerentanan, dan keterlibatan aktif [19].

Penelitian ini menjadi penting karena masih terbatasnya studi empiris di konteks mahasiswa Indonesia yang secara eksplisit menguji peran *cybersecurity engagement* sebagai mediator antara *threat appraisal* dan *security awareness*. Sebagian besar penelitian sebelumnya cenderung memposisikan *security awareness* sebagai variabel independen atau hanya menguji hubungan langsung antara faktor risiko dan perilaku keamanan. Dengan menempatkan *security awareness* sebagai variabel dependen utama dan memasukkan *engagement* sebagai mediator, penelitian ini menawarkan kontribusi konseptual yang lebih mendalam dan kontekstual.

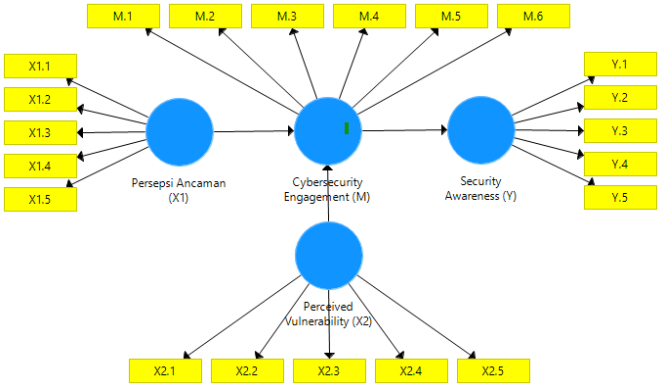
Selain itu, konteks responden yang melibatkan mahasiswa Universitas Negeri Padang dengan rentang usia 18–24 tahun memberikan relevansi praktis yang tinggi, mengingat kelompok usia ini merupakan pengguna aktif teknologi digital sekaligus calon tenaga kerja di era ekonomi digital. Hasil penelitian diharapkan dapat menjadi dasar bagi pengembangan program edukasi keamanan siber yang tidak hanya berfokus pada peningkatan pengetahuan, tetapi juga pada peningkatan persepsi risiko, rasa kerentanan, dan keterlibatan aktif mahasiswa.

Secara keseluruhan, penelitian ini bertujuan untuk menganalisis pengaruh persepsi ancaman dan *perceived vulnerability* terhadap *security awareness* dengan peran mediasi *cybersecurity engagement*. Dengan mengintegrasikan kerangka *Protection Motivation Theory* dan pendekatan keterlibatan aktif, penelitian ini diharapkan mampu memberikan kontribusi teoretis dan praktis dalam upaya meningkatkan kesadaran keamanan siber di kalangan mahasiswa.

Kerangka konseptual penelitian ini disusun untuk menggambarkan hubungan antar variabel yang menjelaskan pembentukan *security awareness* pada mahasiswa dalam konteks keamanan siber. Model penelitian menempatkan

persepsi ancaman dan *perceived vulnerability* sebagai variabel independen yang merepresentasikan penilaian individu terhadap risiko dan kerentanan keamanan digital. Kedua variabel tersebut dipandang sebagai faktor awal yang mendorong respons individu terhadap potensi ancaman siber.

Hubungan antar variabel dalam penelitian ini dirumuskan dalam bentuk model konseptual yang disajikan pada Gambar 1, yang menunjukkan jalur pengaruh langsung dari persepsi ancaman dan *perceived vulnerability* terhadap *cybersecurity engagement*, serta jalur pengaruh tidak langsung terhadap *security awareness* melalui variabel mediasi tersebut.



Gambar 1. Model Konseptual Pengaruh Persepsi Ancaman dan *Perceived vulnerability* terhadap *Security awareness* melalui *Cybersecurity engagement*

Berdasarkan hubungan antar variabel yang digambarkan dalam model konseptual tersebut, penelitian ini selanjutnya merumuskan hipotesis untuk menguji secara empiris pengaruh langsung dan tidak langsung antar konstruk yang diteliti. Hipotesis disusun untuk mengevaluasi peran persepsi ancaman dan *perceived vulnerability* dalam mendorong *cybersecurity engagement*, serta untuk menilai bagaimana *cybersecurity engagement* berkontribusi terhadap pembentukan *security awareness*. Selain itu, hipotesis juga dirumuskan untuk menguji peran *cybersecurity engagement* sebagai variabel mediasi dalam hubungan antara variabel independen dan *security awareness*. Berikut ringkasan hipotesis penelitian ini:

H1: Persepsi ancaman berpengaruh positif terhadap *cybersecurity engagement*.

H2: *Perceived vulnerability* berpengaruh positif terhadap *cybersecurity engagement*.

H3: *Cybersecurity engagement* berpengaruh positif terhadap *security awareness*.

H4: *Cybersecurity engagement* memediasi pengaruh persepsi ancaman terhadap *security awareness*.

H5: *Cybersecurity engagement* memediasi pengaruh *perceived vulnerability* terhadap *security awareness*.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain survei eksplanatori, yang bertujuan untuk menguji hubungan kausal antar konstruk dalam model penelitian. Pendekatan ini dipilih karena sesuai untuk menjelaskan mekanisme pengaruh persepsi ancaman dan *perceived vulnerability* terhadap *security awareness*, dengan *cybersecurity engagement* sebagai variabel mediasi. Desain eksplanatori memungkinkan peneliti menguji tidak hanya hubungan langsung antar variabel, tetapi juga peran variabel antara dalam menjembatani proses kognitif dan perilaku keamanan siber pada individu.

Populasi dalam penelitian ini adalah seluruh mahasiswa Universitas Negeri Padang (UNP) yang berada pada rentang usia 18–24 tahun, yaitu kelompok usia yang secara aktif menggunakan teknologi digital dalam kegiatan akademik maupun non-akademik. Kelompok ini dipilih karena mahasiswa merupakan pengguna intensif layanan digital, media sosial, dan sistem informasi berbasis internet, sehingga memiliki tingkat paparan risiko keamanan siber yang relatif tinggi.

Teknik pengambilan sampel yang digunakan adalah non-probability sampling dengan pendekatan *purposive sampling*. Responden dipilih berdasarkan kriteria:

1. berstatus sebagai mahasiswa aktif Universitas Negeri Padang,
2. berada pada rentang usia 18–24 tahun, dan
3. menggunakan teknologi digital serta internet secara rutin dalam aktivitas sehari-hari.

Jumlah responden yang berpartisipasi dalam penelitian ini adalah 134 mahasiswa, terdiri dari 60 responden laki-laki dan 74 responden perempuan. Jumlah sampel ini dinilai memadai untuk analisis model struktural berbasis variabel laten, khususnya dalam pendekatan *Partial Least Squares–Structural Equation Modeling* (PLS-SEM), yang relatif toleran terhadap ukuran sampel menengah.

Penelitian ini dilaksanakan dalam rentang waktu Agustus 2025 hingga November 2025. Proses penelitian meliputi tahap persiapan instrumen, penyebaran kuesioner, pengumpulan data, serta pengolahan dan analisis data. Seluruh proses pengumpulan data dilakukan secara daring menggunakan kuesioner berbasis online form, mengingat karakteristik responden yang akrab dengan teknologi digital.

Penelitian ini melibatkan empat konstruk utama, yaitu dua variabel independen, satu variabel mediasi, dan satu variabel dependen. Seluruh konstruk diukur menggunakan indikator reflektif yang disusun berdasarkan kajian literatur dan disesuaikan dengan konteks mahasiswa.

1. Persepsi Ancaman (X1)
   Persepsi ancaman diukur menggunakan 5 indikator yang mencerminkan persepsi responden terhadap meningkatnya ancaman kejahatan siber, kesadaran akan risiko akibat kelalaian pribadi, pandangan terhadap *hacker* dan penipu online sebagai ancaman nyata, kewaspadaan terhadap kemungkinan terjadinya serangan siber, serta tingkat keseriusan ancaman keamanan siber.
2. *Perceived vulnerability* (X2)
   Perceived vulnerability diukur menggunakan 5 indikator yang merepresentasikan keyakinan responden mengenai kerentanan akun digital, ketidakamanan data pribadi, potensi menjadi korban penipuan online, adanya celah dalam pertahanan keamanan digital, serta persepsi kerentanan diri terhadap ancaman di internet.
3. *Cybersecurity engagement* (M)
   Cybersecurity engagement diukur menggunakan 5 indikator yang mencerminkan keterlibatan aktif responden dalam mencari informasi keamanan siber, memperbarui atau mengganti kata sandi, mengikuti pelatihan atau kegiatan edukatif terkait keamanan siber, berdiskusi dengan orang lain mengenai keamanan digital, serta mengambil inisiatif mandiri untuk meningkatkan keamanan perangkat dan akun.
4. *Security awareness* (Y)

Security awareness diukur menggunakan 5 indikator yang mencakup kesadaran terhadap risiko aktivitas online, pengetahuan mengenai metode kejahatan siber, pemahaman akan pentingnya menjaga kerahasiaan kata sandi, kesadaran terhadap risiko membagikan informasi pribadi di media sosial, serta kesadaran akan peran dan tanggung jawab personal dalam menjaga keamanan siber.

Instrumen penelitian berupa kuesioner tertutup yang disusun dalam bentuk pernyataan dengan skala Likert lima tingkat, mulai dari sangat tidak setuju (1) hingga sangat setuju (5). Seluruh butir pernyataan dirancang untuk mengukur persepsi dan pengalaman responden secara subjektif terkait keamanan siber.

Sebelum disebarkan secara luas, instrumen ditelaah secara konseptual untuk memastikan kesesuaian indikator dengan definisi operasional masing-masing variabel. Penyebaran kuesioner dilakukan secara daring untuk memudahkan akses responden dan meningkatkan tingkat partisipasi.

Data yang terkumpul dianalisis menggunakan pendekatan *Partial Least Squares–Structural Equation Modeling* (PLS-SEM). Metode ini dipilih karena sesuai untuk:

1. Model penelitian dengan variabel laten dan indikator reflektif,
2. Tujuan penelitian yang bersifat prediktif dan eksplanatori, serta
3. Ukuran sampel yang relatif menengah.

Tahapan analisis dalam penelitian ini meliputi evaluasi model pengukuran dan evaluasi model struktural menggunakan pendekatan *Partial Least Squares–Structural Equation Modeling* (PLS-SEM).

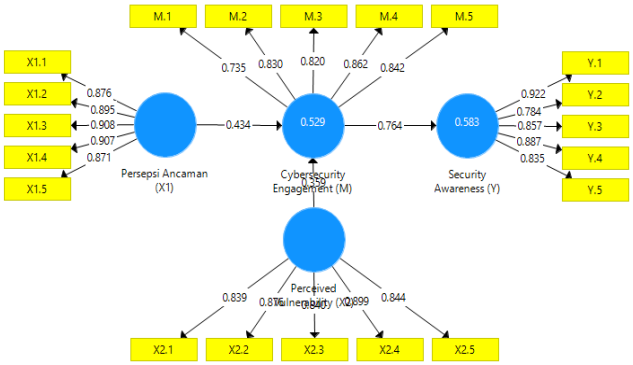
1. Evaluasi Model Pengukuran (*Measurement Model*)
   Evaluasi model pengukuran dilakukan untuk menilai kualitas instrumen penelitian, yang meliputi:
   a. Validitas konvergen, yang dievaluasi melalui nilai *outer loading* ($\geqslant$ 0,70) dan *Average Variance Extracted* (AVE $\geqslant$ 0,50),
   b. Reliabilitas konstruk, yang diuji menggunakan nilai *Cronbach's Alpha*, *rho_A*, dan *Composite Reliability* ($\geqslant$ 0,70),
   c. Validitas diskriminan, yang diuji menggunakan kriteria Fornell–Larcker,
   d. Uji multikolinearitas, yang dilakukan melalui nilai *Variance Inflation Factor* (VIF) (< 5).
2. Evaluasi Model Struktural (*Structural Model*)
   Evaluasi model struktural dilakukan untuk menguji hubungan antar konstruk dalam model penelitian, yang meliputi:
   a. Koefisien jalur (*path coefficients*) untuk melihat arah dan kekuatan pengaruh antar variabel,
   b. Koefisien determinasi (R^2 dan R^2 *Adjusted*) untuk mengukur kemampuan model dalam menjelaskan variabel endogen,
3. Uji Signifikansi Hipotesis (*Bootstrapping*)
   Pengujian hipotesis dalam penelitian ini dilakukan berdasarkan hasil evaluasi model struktural. Hipotesis H1 hingga H3 diuji melalui analisis pengaruh langsung antar konstruk menggunakan nilai koefisien jalur, *t-statistic*, dan *p-value* yang diperoleh dari prosedur *Bootstrapping*. Selanjutnya, hipotesis H4 dan H5 diuji melalui analisis pengaruh tidak langsung untuk menilai peran *cybersecurity engagement* sebagai variabel mediasi. Hipotesis dinyatakan diterima apabila nilai *t-statistic* lebih besar dari 1,96 dan nilai *p-value* kurang dari 0,05.
4. Uji Efek Mediasi
   Pengujian efek mediasi dilakukan untuk mengevaluasi peran *cybersecurity engagement* sebagai variabel mediasi dalam hubungan antara persepsi ancaman dan *perceived vulnerability* terhadap *security awareness*. Efek mediasi diuji melalui analisis pengaruh tidak langsung (*indirect effect*) menggunakan prosedur *Bootstrapping*. Mediasi dinyatakan signifikan apabila nilai pengaruh tidak langsung memiliki *t-statistic* > 1,96 dan *p-value* < 0,05.

III. HASIL DAN PEMBAHASAN

A. Evaluasi Model Pengukuran (*Measurement Model*)

Evaluasi model pengukuran dilakukan untuk menilai sejauh mana indikator-indikator yang digunakan mampu mengukur konstruk laten secara valid dan reliabel. Pada penelitian ini, evaluasi model pengukuran mencakup pengujian validitas konvergen, validitas diskriminan, reliabilitas konstruk, serta uji multikolinearitas antar indikator. Pengujian ini bertujuan untuk memastikan bahwa setiap konstruk dalam model penelitian telah memenuhi kriteria kualitas pengukuran sebelum dilakukan analisis lebih lanjut pada model struktural.

Hasil evaluasi awal model pengukuran dan model struktural ditunjukkan pada Gambar 2, yang menyajikan nilai *outer loading* setiap indikator, koefisien jalur antar konstruk, serta nilai koefisien determinasi (R^2) pada variabel endogen.



Gambar 2. Model PLS-SEM dengan Nilai *Outer loading*, Koefisien Jalur, dan R^2

Berdasarkan Gambar 2, seluruh indikator pada masing-masing konstruk memiliki nilai *outer loading* di atas batas minimum yang direkomendasikan, yang menunjukkan bahwa indikator-indikator tersebut mampu merepresentasikan konstruk laten yang diukur. Selain itu, nilai R^2 pada konstruk *cybersecurity engagement* dan *security awareness* menunjukkan kemampuan model yang memadai dalam menjelaskan variasi variabel endogen.

Tabel 1.
Nilai *Outer loading* Indikator pada Model PLS

Konstruk	Indikator	*Outer loading*
Persepsi Ancaman (X1)	X1.1	0.876
	X1.2	0.895
	X1.3	0.908
	X1.4	0.907
	X1.5	0.871
Perceived vulnerability (X2)	X2.1	0.839
	X2.2	0.876
	X2.3	0.840
	X2.4	0.899
	X2.5	0.844
Cybersecurity engagement (M)	M.1	0.735
	M.2	0.830
	M.3	0.826
	M.4	0.862
	M.5	0.842
Security awareness (Y)	Y.1	0.922
	Y.2	0.784
	Y.3	0.857
	Y.4	0.887
	Y.5	0.835

Berdasarkan Tabel 1, seluruh indikator pada masing-masing konstruk memiliki nilai *outer loading* di atas batas minimum 0,70. Hasil ini menunjukkan bahwa seluruh indikator mampu merepresentasikan konstruk laten yang diukur secara memadai, sehingga memenuhi kriteria validitas konvergen.

Pengujian reliabilitas konstruk dan validitas konvergen pada tingkat konstruk dilakukan menggunakan nilai *Cronbach's Alpha*, *rho_A*, *Composite Reliability*, dan *Average Variance Extracted* (AVE). Hasil pengujian tersebut disajikan pada tabel berikut.

Tabel 2.
Hasil Uji Reliabilitas Konstruk dan *Average Variance Extracted* (AVE)

Construct	*Cronbach's Alpha*	*rho_A*	*Composite Reliability*	*Average Variance Extracted* (AVE)
Cybersecurity engagement (M)	0.877	0.888	0.910	0.671
Perceived vulnerability (X2)	0.912	0.917	0.934	0.740
Persepsi Ancaman (X1)	0.935	0.936	0.951	0.795
Security awareness (Y)	0.910	0.914	0.933	0.737

Berdasarkan Tabel 2, seluruh konstruk memiliki nilai *Cronbach's Alpha*, *rho_A*, dan *Composite Reliability* di atas batas minimum 0,70, serta nilai AVE di atas 0,50. Hasil ini menunjukkan bahwa seluruh konstruk dalam penelitian ini memenuhi kriteria reliabilitas dan validitas konvergen yang memadai, sehingga layak digunakan dalam analisis model struktural.

Validitas diskriminan dalam penelitian ini diuji menggunakan kriteria *Fornell–Larcker* untuk memastikan bahwa setiap konstruk laten memiliki perbedaan yang memadai satu sama lain. Pengujian ini dilakukan dengan membandingkan nilai akar kuadrat *Average Variance Extracted* (AVE) pada setiap konstruk dengan nilai korelasi antar konstruk. Hasil pengujian validitas diskriminan disajikan pada tabel berikut.

Tabel 3.
Hasil Uji Validitas Diskriminan Berdasarkan Kriteria Fornell–Larcker.

Construct	*Cybersecurity engagement* (M)	*Perceived vulnerability* (X2)	Persepsi Ancaman (X1)	*Security awareness* (Y)
Cybersecurity engagement (M)	0.819			
Perceived vulnerability (X2)	0.654	0.860		
Persepsi Ancaman (X1)	0.678	0.679	0.892	
Security awareness (Y)	0.764	0.709	0.840	0.858

Berdasarkan Tabel 3, nilai akar kuadrat AVE pada setiap konstruk lebih tinggi dibandingkan dengan nilai korelasi antara konstruk tersebut dengan konstruk lainnya. Hasil ini menunjukkan bahwa masing-masing konstruk memiliki validitas diskriminan yang baik, sehingga dapat disimpulkan bahwa konstruk-konstruk dalam model penelitian saling berbeda secara konseptual.

Uji multikolinearitas dilakukan untuk memastikan bahwa tidak terdapat korelasi yang tinggi antar indikator maupun antar konstruk dalam model penelitian. Pengujian multikolinearitas dalam penelitian ini dilakukan menggunakan nilai *Variance Inflation Factor (VIF)*. Hasil uji multikolinearitas disajikan pada tabel berikut.

Tabel 4.
Ringkasan Hasil Uji Multikolinearitas Berdasarkan Nilai *Variance Inflation Factor* (VIF)

Konstruk	VIF Minimum	VIF Maksimum	Status
Cybersecurity engagement (M)	1.783	2.959	Tidak ada multikolinearitas
Persepsi Ancaman (X1)	2.826	3.908	Tidak ada multikolinearitas
Perceived vulnerability (X2)	2.222	3.568	Tidak ada multikolinearitas
Security awareness (Y)	1.815	4.273	Tidak ada multikolinearitas

Berdasarkan Tabel 4, seluruh indikator memiliki nilai VIF di bawah batas maksimum yang direkomendasikan, yaitu 5. Hasil ini menunjukkan bahwa tidak terdapat masalah multikolinearitas dalam model penelitian, sehingga indikator-indikator yang digunakan dinyatakan bebas dari korelasi tinggi dan layak digunakan untuk analisis lebih lanjut.

B. Evaluasi Model Struktural

Evaluasi model struktural dilakukan untuk menilai hubungan antar konstruk laten dalam model penelitian serta kemampuan model dalam menjelaskan variabel endogen. Pada tahap ini, evaluasi difokuskan pada analisis koefisien determinasi, koefisien jalur, dan signifikansi pengaruh antar variabel untuk menguji hipotesis penelitian yang telah dirumuskan.

Koefisien determinasi (R^2) digunakan untuk menilai kemampuan model struktural dalam menjelaskan variabel endogen. Nilai R^2 menunjukkan proporsi variasi variabel endogen yang dapat dijelaskan oleh variabel eksogen dalam model penelitian. Hasil pengujian koefisien determinasi disajikan pada tabel berikut.

Tabel 5.
Nilai Koefisien Determinasi (R^2 dan R^2 *Adjusted*).

Konstruk Endogen	R Square (R^2)	R Square *Adjusted*
Cybersecurity engagement (M)	0.529	0.522
Security awareness (Y)	0.583	0.580

Berdasarkan Tabel 5, nilai R^2 untuk konstruk *cybersecurity engagement* sebesar 0,529, yang menunjukkan bahwa persepsi ancaman dan *perceived vulnerability* mampu menjelaskan 52,9% variasi *cybersecurity engagement*. Selanjutnya, nilai R^2 untuk konstruk *security awareness* sebesar 0,583, yang menunjukkan bahwa *cybersecurity engagement* mampu menjelaskan 58,3% variasi *security awareness*. Hasil ini mengindikasikan bahwa model struktural memiliki kemampuan penjelasan yang moderat dan memadai.

Koefisien jalur (*path coefficients*) digunakan untuk menunjukkan arah dan kekuatan pengaruh antar konstruk dalam model struktural. Nilai koefisien jalur menggambarkan sejauh mana perubahan pada variabel eksogen memengaruhi variabel endogen. Hasil estimasi koefisien jalur dalam model penelitian ini disajikan pada tabel berikut.

Tabel 6.
Nilai Koefisien Jalur (*Path coefficients*) Model Struktural

Hubungan Antar Konstruk	Path Coefficient (β)
Perceived vulnerability (X2) → *Cybersecurity engagement* (M)	0.359
Persepsi Ancaman (X1) → *Cybersecurity engagement* (M)	0.434
Cybersecurity engagement (M) → *Security awareness* (Y)	0.764

Berdasarkan Tabel 6, persepsi ancaman memiliki pengaruh positif terhadap *cybersecurity engagement* dengan nilai koefisien jalur sebesar 0,434, sedangkan *perceived vulnerability* juga menunjukkan pengaruh positif terhadap *cybersecurity engagement* dengan nilai koefisien jalur sebesar 0,359. Selanjutnya, *cybersecurity engagement* berpengaruh positif terhadap *security awareness* dengan nilai koefisien jalur sebesar 0,764. Hasil ini menunjukkan bahwa seluruh hubungan antar konstruk dalam model memiliki arah pengaruh yang positif.

C. Uji Signifikansi Hipotesis (*Bootstrapping*)

Pengujian signifikansi hipotesis dalam penelitian ini dilakukan menggunakan prosedur *Bootstrapping* untuk mengevaluasi pengaruh langsung antar konstruk dalam model struktural. Signifikansi hubungan diuji berdasarkan nilai *t-statistic* dan *p-value*, dengan kriteria nilai *t-statistic* > 1,96 dan *p-value* < 0,05. Hasil pengujian pengaruh langsung antar variabel disajikan pada tabel berikut.

Tabel 7.
Hasil Uji Signifikansi Pengaruh Langsung Berdasarkan *Bootstrapping*

Path	β	STDEV	t-value	*p-value*
Cybersecurity engagement (M) → *Security awareness* (Y)	0.764	0.044	17.741	0.000
Perceived vulnerability (X2) → *Cybersecurity engagement* (M)	0.359	0.100	3.593	0.000
Persepsi Ancaman (X1) → *Cybersecurity engagement* (M)	0.434	0.085	5.116	0.000

Berdasarkan Tabel 7, *cybersecurity engagement* berpengaruh positif dan signifikan terhadap *security awareness* dengan nilai koefisien jalur sebesar 0,764 (t = 17,471; p < 0,05). Selanjutnya, *perceived vulnerability* berpengaruh positif dan signifikan terhadap *cybersecurity engagement* dengan nilai koefisien jalur sebesar 0,359 (t = 3,593; p < 0,05), dan persepsi ancaman juga berpengaruh positif dan signifikan terhadap *cybersecurity engagement* dengan nilai koefisien jalur sebesar 0,434 (t = 5,116; p < 0,05). Hasil ini menunjukkan bahwa seluruh pengaruh langsung dalam model penelitian terbukti signifikan, sehingga hipotesis H1, H2, dan H3 diterima.

D. Uji Efek Mediasi

Pengujian efek mediasi dalam penelitian ini dilakukan untuk menilai peran *cybersecurity engagement* sebagai variabel mediasi dalam hubungan antara persepsi ancaman dan *perceived vulnerability* terhadap *security awareness*. Efek mediasi diuji menggunakan prosedur *Bootstrapping* melalui analisis total *indirect effect*s. Hasil pengujian efek tidak langsung disajikan pada tabel berikut.

Tabel 8.
Hasil Uji Efek Mediasi Berdasarkan Total *Indirect effect*s

Relationship	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Perceived vulnerability (X2) → *Security awareness* (Y)	0.274	0.280	0.084	3.265	0.001
Persepsi Ancaman (X1) → *Security awareness* (Y)	0.331	0.330	0.071	4.687	0.000

Berdasarkan Tebel 8, hasil pengujian menunjukkan bahwa *perceived vulnerability* berpengaruh positif dan signifikan terhadap *security awareness* melalui *cybersecurity engagement* dengan nilai efek tidak langsung sebesar 0,274 (t = 3,265; p < 0,05). Selain itu, persepsi ancaman juga berpengaruh positif dan signifikan terhadap *security awareness* melalui *cybersecurity engagement* dengan nilai efek tidak langsung sebesar 0,331 (t = 4,687; p < 0,05). Hasil ini menunjukkan bahwa *cybersecurity engagement* berperan sebagai variabel mediasi, sehingga hipotesis H4 dan H5 diterima.

Ringkasan hasil pengujian hipotesis dalam penelitian ini disajikan untuk memberikan gambaran komprehensif mengenai hubungan antar variabel yang diuji dalam model struktural. Pengujian hipotesis dilakukan berdasarkan nilai

koefisien jalur, *t-statistic*, dan *p-value* yang diperoleh dari prosedur *Bootstrapping*. Tabel 9 berikut merangkum hasil pengujian hipotesis H1 hingga H5, baik untuk pengaruh langsung maupun pengaruh tidak langsung (mediasi).

Tabel 9.
Ringkasan Hasil Pengujian Hipotesis

Hipotesis	Hubungan Antar Variabel	Koefisien Jalur (β)	*t-statistic*	*p-value*	Keputusan
H1	Persepsi Ancaman → *Cybersecurity engagement*	0.434	5.116	0.000	Diterima
H2	*Perceived vulnerability* → *Cybersecurity engagement*	0.359	3.593	0.000	Diterima
H3	*Cybersecurity engagement* → *Security awareness*	0.764	17.471	0.000	Diterima
H4	Persepsi Ancaman → *Cybersecurity engagement* → *Security awareness*	0.331	4.687	0.000	Diterima
H5	*Perceived vulnerability* → *Cybersecurity engagement* → *Security awareness*	0.274	3.265	0.001	Diterima

E. Pembahasan

Hasil penelitian menunjukkan bahwa pembentukan *security awareness* pada mahasiswa dipengaruhi oleh kombinasi persepsi risiko dan keterlibatan aktif dalam aktivitas keamanan siber. Temuan ini menegaskan bahwa kesadaran keamanan tidak muncul secara pasif, melainkan berkembang melalui respons individu terhadap ancaman dan rasa kerentanan yang dirasakan.

Pengaruh positif persepsi ancaman terhadap *cybersecurity engagement* menunjukkan bahwa mahasiswa yang memandang ancaman siber sebagai sesuatu yang nyata dan serius cenderung lebih terlibat dalam upaya menjaga keamanan digital. Persepsi terhadap keberadaan dan intensitas ancaman mendorong mahasiswa untuk lebih waspada serta aktif mencari dan menerapkan praktik keamanan siber dalam kehidupan sehari-hari.

Selain itu, *perceived vulnerability* juga terbukti mendorong *cybersecurity engagement*. Rasa kerentanan personal membuat mahasiswa tidak hanya menyadari risiko secara umum, tetapi juga memandang risiko tersebut sebagai ancaman yang dapat berdampak langsung pada dirinya. Kondisi ini memicu keterlibatan yang lebih aktif dalam aktivitas keamanan siber sebagai bentuk perlindungan diri.

Hasil penelitian juga menunjukkan bahwa *cybersecurity engagement* berpengaruh positif terhadap *security awareness*. Keterlibatan aktif dalam aktivitas keamanan siber memperkuat pemahaman, kewaspadaan, dan rasa tanggung jawab mahasiswa terhadap keamanan digital. Dengan demikian, *security awareness* terbentuk melalui praktik dan pengalaman yang berkelanjutan, bukan hanya melalui pengetahuan teoritis.

Lebih lanjut, peran mediasi *cybersecurity engagement* menegaskan bahwa pengaruh persepsi ancaman dan *perceived vulnerability* terhadap *security awareness* terjadi melalui mekanisme keterlibatan aktif. Temuan ini menunjukkan bahwa peningkatan kesadaran keamanan siber pada mahasiswa akan lebih efektif apabila tidak hanya menekankan aspek persepsi risiko, tetapi juga mendorong partisipasi aktif dalam aktivitas keamanan siber.

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa *security awareness* pada mahasiswa dibentuk melalui interaksi antara persepsi ancaman, *perceived vulnerability*, dan keterlibatan aktif dalam aktivitas keamanan siber (*cybersecurity engagement*). Persepsi terhadap ancaman siber dan rasa kerentanan personal terbukti mendorong mahasiswa untuk lebih terlibat dalam praktik keamanan digital, yang pada akhirnya memperkuat tingkat kesadaran keamanan siber.

Temuan penelitian menunjukkan bahwa *cybersecurity engagement* memainkan peran penting sebagai mekanisme mediasi yang menjembatani pengaruh persepsi risiko terhadap *security awareness*. Hal ini menegaskan bahwa peningkatan kesadaran keamanan siber tidak cukup hanya dengan meningkatkan persepsi ancaman atau pemahaman risiko, tetapi perlu disertai dengan upaya mendorong keterlibatan aktif mahasiswa dalam aktivitas keamanan siber.

Secara praktis, hasil penelitian ini mengindikasikan bahwa institusi pendidikan tinggi perlu mengembangkan strategi peningkatan keamanan siber yang tidak hanya berfokus pada penyampaian informasi, tetapi juga pada penguatan partisipasi aktif mahasiswa melalui kegiatan edukatif dan pengalaman praktis. Penelitian selanjutnya disarankan untuk melibatkan sampel yang lebih luas serta mengeksplorasi variabel lain yang berpotensi memengaruhi *security awareness* dalam konteks keamanan siber.

DAFTAR PUSTAKA

[1] L. M. Ganiem, R. Setiawati, S. Suardi, N. Nurhayai, and R. Ramdhani, "Society in the Digital Era: Adaptation, Change, and Response to Communication Technology," J. Int. Dakwah Commun., vol. 4, no. 1, pp. 123–135, June 2024, doi: 10.55849/jidc.v4i1.639.

[2] K. Martzoukou, C. Fulton, P. Kostagiolas, and C. Lavranos, "A study of higher education students' self-perceived digital competences for learning and everyday life online participation," J. Doc., vol. 76, no. 6, pp. 1413–1458, June 2020, doi: 10.1108/JD-03-2020-0041.

[3] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," Sensors, vol. 23, no. 15, p. 6666, July 2023, doi: 10.3390/s23156666.

[4] A. K. Gwenhure, "University students' security behavior against email phishing attacks: insights from the health belief model," J. Cybersecurity, vol. 11, no. 1, p. tyaf034, Jan. 2025, doi: 10.1093/cybsec/tyaf034.

[5] K. Okokpujie, M. A. Ariyo, F. S. Moninuola, M. B. Akanle, and I. P. Okokpujie, "Evaluating Students' Vulnerability and Awareness to Phishing Attacks in Educational Institutions," Int. J. Saf. Secur. Eng., vol. 15, no. 3, pp. 621–630, Mar. 2025, doi: 10.18280/ijsse.150320.

[6] I. Dunđer, S. Seljan, and M. Odak, "Information Security awareness in the University Environment: A Focus on

Undergraduates," TEM J., pp. 1621–1628, May 2025, doi: 10.18421/TEM142-59.
[7] M. A. Alqahtani, "Factors Affecting Cybersecurity awareness among University Students," Appl. Sci., vol. 12, no. 5, p. 2589, Mar. 2022, doi: 10.3390/app12052589.
[8] K. Wang, X. Guo, and D. Yang, "Research on the Effectiveness of Cyber Security awareness in ICS Risk Assessment Frameworks," Electronics, vol. 11, no. 10, p. 1659, May 2022, doi: 10.3390/electronics11101659.
[9] D. Fischer-Preßler, D. Bonaretti, and K. Fischbach, "A Protection-Motivation Perspective to Explain Intention to Use and Continue to Use Mobile Warning Systems," Bus. Inf. Syst. Eng., vol. 64, no. 2, pp. 167–182, Apr. 2022, doi: 10.1007/s12599-021-00704-0.
[10] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," Information, vol. 13, no. 9, p. 413, Aug. 2022, doi: 10.3390/info13090413.
[11] M. A. Alqahtani, "Factors Affecting Cybersecurity awareness among University Students," Appl. Sci., vol. 12, no. 5, p. 2589, Mar. 2022, doi: 10.3390/app12052589.
[12] W. Li, R. Liu, L. Sun, Z. Guo, and J. Gao, "An Investigation of Employees' Intention to Comply with Information Security System—A Mixed Approach Based on Regression Analysis and fsQCA," Int. J. Environ. Res. Public. Health, vol. 19, no. 23, p. 16038, Nov. 2022, doi: 10.3390/ijerph192316038.
[13] K. C. Ng, X. Zhang, J. Y. L. Thong, and K. Y. Tam, "Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective," J. Manag. Inf. Syst., vol. 38, no. 3, pp. 732–764, July 2021, doi: 10.1080/07421222.2021.1962601.
[14] A. Alqarni, "The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: the mediating role of cyber threat perception and the moderating role of internet usage duration," Humanit. Soc. Sci. Commun., vol. 12, no. 1, p. 1837, Nov. 2025, doi: 10.1057/s41599-025-06122-x.
[15] E. R. Noble, T. F. Ask, and B. J. Knox, "Tailored Extended Reality Environments for Education and Training in Cybersecurity: Engagement Beyond Awareness," in 2025 IEEE Global Engineering Education Conference (EDUCON), London, United Kingdom: IEEE, Apr. 2025, pp. 1–9. doi: 10.1109/EDUCON62633.2025.11016494.
[16] J. C. Tise and M. M. McGill, "Validation of an Instrument to Measure Self-Efficacy in Information Security," in Proceedings of the 2024 on ACM Virtual Global Computing Education Conference V. 1, Virtual Event NC USA: ACM, Dec. 2024, pp. 214–220. doi: 10.1145/3649165.3690095.
[17] E. R. Noble, T. F. Ask, and B. J. Knox, "Tailored Extended Reality Environments for Education and Training in Cybersecurity: Engagement Beyond Awareness," in 2025 IEEE Global Engineering Education Conference (EDUCON), London, United Kingdom: IEEE, Apr. 2025, pp. 1–9. doi: 10.1109/EDUCON62633.2025.11016494.
[18] C. Z. Oroni, F. Xianping, D. D. Ndunguru, and A. Ani, "Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis," Comput. Secur., vol. 150, p. 104276, Mar. 2025, doi: 10.1016/j.cose.2024.104276.