Analisis Kesadaran *Cyber Security* pada Kalangan Pelaku *e-Commerce* di Indonesia

Galih Rahmadi
Program Studi Informatika
Fakultas Teknologi Industri UII
Yogyakarta
16523077@students.uii.ac.id

Ahmad Raf'ie Pratama
Program Studi Informatika
Fakultas Teknologi Industri UII
Yogyakarta
ahmad.rafie@uii.ac.id

***Abstrak*—Hadirnya *e-commerce* di Indonesia sebagai aktivitas jual beli barang atau jasa melalui internet memungkinkan dapat terjadinya *cybercrime*. Ancaman terjadinya *cybercrime* merupakan hal yang dapat mengganggu aktivitas *e-commerce*, sehingga konsumen maupun pelaku usaha harus mampu melindungi dari ancaman tersebut dengan *cyber security*. Maka peneliti berusaha melakukan penelitian terkait faktor-faktor apa saja yang mempengaruhi kesadaran *cyber security* pada kalangan pelaku *e-commerce* terhadap ancaman *cybercrime*. Analisis data ini menggunakan sumber data primer dari hasil kuisioner yang dibagikan kepada pengguna *e-commerce*. Penelitian ini menggunakan teknik *Structural Equation Modeling* (SEM), untuk mengukur hubungan antar variabel laten berupa pengetahuan dan kesadaran *cyber security* dengan demografi pengguna *e-commerce*. Hasil penelitian menunjukkan bahwa variabel pengetahuan *cyber security* terdapat hubungan yang memiliki sifat signifikan terhadap kesadaran *cyber security* pelaku *e-commerce* dan variabel jenis kelamin memiliki hubungan bersifat signifikan terhadap pengetahuan *cyber security* yang secara tidak langsung berpengaruh pada kesadaran *cyber security*.**

Kata Kunci—cyber security, e-commerce, Structural Equation Modeling, kesadaran, pengetahuan.

I. PENDAHULUAN

Pada era disrupsi ini membuat pelaku usaha selalu membuat suatu inovasi agar dapat beradaptasi terhadap kegiatan perdagangan pelaku *e-commerce* agar memberikan kelancaran dalam proses bisnis sehingga dapat bersaing secara kompetitif. Salah satu yang dilakukan pelaku usaha yaitu dengan menggunakan teknologi internet dalam proses bisnis sehingga membuat peralihan dari antar muka ke internet. Teknologi tersebut kita kenal dengan istilah *electronic commerce (e-commerce)* atau perdagangan elektronik. Karena adanya e-*commerce* membuat transaksi menjadi lebih interaktif, mudah, murah, dan cepat dalam mendapatkan produk atau jasa yang masyarakat inginkan. Hal ini lah yang dimanfaatkan pelaku usaha sehingga dapat menciptakan peluang bisnis yang signifikan, meningkatkan akses yang tanpa batas, dan konektivitas dengan skala yang lebih besar dalam lokal maupun skala global [1].

Menurut data GlobalWebIndex (2019), pada Kuartal II 2019 bahwa 90 persen pengguna internet di Indonesia yang berusia antara 16 sampai 64 tahun melaporkan bahwa mereka pernah membeli produk dan layanan *e-commerce* hal ini membuat Indonesia menjadi tingkat pengguna *e-commerce* tertinggi di dunia [2]. Berkembangnya *e-commerce* di Indonesia diprediksi bakal menyentuh angka 189,2 juta pada 2023, hal tersebut naik sekitar 25 persen dari tahun 2019 yang sebesar 112,1 juta pengguna [3].

Banyaknya pengguna *e-commerce* di Indonesia yang memanfaatkannya sebagai aktivitas pembelian atau penjualan produk melalui internet, karena pengguna dapat berkomunikasi dengan menyamarkan identitasnya, tanpa dibatasi oleh batas wilayah, dan bahkan lintas negara, sehingga hal tersebut dapat memungkinkan dapat terjadinya ancaman *cybercrime* [4]. Ancaman terjadinya *cybercrime* merupakan hal serius yang dapat mengganggu aktivitas *e-commerce*. Maka, konsumen maupun pelaku usaha harus dapat melindungi dirinya dari ancaman tersebut dengan *cyber security*.

Cyber security yaitu sebagai mekanisme untuk mendeteksi celah keamanan komputer, mencegah ancaman kejahatan komputer, dan pemulihan kembali komputer atau perangkat yang telah terkena serangan siber [5]. Hal ini sangat dibutuhkan karena telah berkembangnya penggunaan teknologi internet, khususnya pada *e-commerce* yang rentan terhadap *cybercrime*. Dalam praktiknya, *cybercrime* menargetkan kelemahan dari suatu komputer atau perangkat dengan memanfaatkan internet dengan tujuan untuk melakukan jenis kejahatan yang diinginkan pelaku kejahatan.

Di Indonesia untuk kasus *cybercrime* dapat dibuktikan oleh temuan Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri yang menerima 4.586 laporan sepanjang Januari-Desember 2019. Laporan soal penipuan online yang terjadi paling mendominasi nomor dua, yakni sebanyak 1.617 kasus [6]. Korban pada *cybercrime* biasanya terjadi pada pengguna atau pelaku *e-commerce* itu sendiri yaitu pembeli dan penjual. Sehingga ini dapat dijadikan catatan penting terkait tingkat kesadaran akan *cyber security* di Indonesia.

Penciptaan malware yang paling berbahaya adalah ketika peretas (individu atau kelompok) membuat program perangkat lunak berbahaya dalam upaya untuk memenuhi tujuan kriminal spesifik demi keuntungan mereka sendiri atau kelompok. Peretas ini menciptakan virus komputer dan program trojan yang dapat

mencuri kode akses ke rekening bank, mengiklankan produk atau layanan di komputer korban secara ilegal menggunakan sumber daya komputer yang terinfeksi untuk mengembangkan dan menjalankan kampanye spam, serangan jaringan terdistribusi (juga disebut serangan DDoS), dan pemerasan korban.

Karena banyaknya permasalahan dan kejahatan yang terjadi pada *e-commerce*, peneliti berupaya mencari faktor-faktor apa saja yang mempengaruhi kesadaran *cyber security* pada kalangan pelaku *e-commerce* di Indonesia dengan menyebarkan kuisioner secara daring, kemudian menggunakan metode statistik untuk melakukan analisis dengan teknik *structural equation modeling* (SEM) yang diharapkan mampu memberikan hasil berupa faktor-faktor tersebut.

II. KAJIAN LITERATUR

A. *E-commerce*

Definisi *e-commerce* adalah pertukaran informasi dan transaksi bisnis demi mempertahankan hubungan bisnis melalui jaringan internet. Menurut Dr. Anil Khurana *e-commerce* sebagai penggunaan komputer, internet dan perangkat lunak untuk mengirim dan menerima spesifikasi dan gambar produk; tawaran, pesanan pembelian, dan faktur; dan segala jenis data lain yang perlu dikomunikasikan kepada pelanggan, pemasok, karyawan, atau publik [7].

B. *Cyber Security*

Cyber Security merupakan praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman. Ini juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik. Istilah ini berlaku dalam berbagai konteks, dari bisnis ke komputasi mobile, dan dapat dibagi menjadi beberapa kategori umum seperti *network security*, *information security*, dan *end-user education* [8].

C. *Pengetahuan dan Kesadaran Cyber Security*

Kesadaran *cyber security* adalah tingkat pemahaman pengguna tentang pentingnya menjaga keamanan informasi dan tanggung jawab mereka serta melakukan kontol terhadap keamanan informasi yang memadai demi melindungi data dan jaringan [9]. Peretas (individu atau kolektif) cenderung mencari pengguna yang paling rentan yaitu mereka yang kurang dalam pengetahuan dan kesadaran *cyber security*.

D. *Structural Equation Modeling (SEM)*

Structural Equation Modeling (SEM) merupakan teknik statistik yang memungkinkan serangkaian hubungan antara satu atau lebih variabel independen (IV) dan satu atau lebih variabel dependen (DV), baik kontinu maupun diskrit, yang kemudian dianalisis. Baik IV maupun DV dapat menjadi faktor atau variabel yang diukur. *Structural Equation Modeling* (SEM) juga disebut sebagai pemodelan kausal, analisis kausal, pemodelan persamaan simultan, analisis struktur kovarian, analisis jalur, atau analisis faktor konfirmatori [10]. Dua yang terakhir sebenarnya adalah tipe khusus dari SEM yang kemudian akan digunakan pada penelitian kali ini.

E. *Penelitian Terdahulu*

1) Penelitian Pertama

Risiko keamanan yang terjadi pada *e-commerce* ini membuat banyak penelitian terdahulu yang mengkaji hal tersebut. Sebagaimana penelitian yang dilakukan oleh Juan Carlos Roca et al. (2008) dengan judul "*The importance of perceived trust, security and privacy in online trading systems"*. Namun, penelitian ini memiliki kekurangan yaitu sampel yang digunakan untuk survei seluruhnya terdiri dari mahasiswa sarjana dalam kursus lanjutan dari satu universitas sehingga tidak mewakili populasi *e-commerce* keseluruhan. Selain itu, penelitian tersebut belum melakukan analisis terpisah terkait dengan pengetahuan dan kesadaran penggunanya. Maka, peneliti mencoba untuk mengambil populasi *e-commerce* secara keseluruhan dan melalukan analisis terpisah terkait dengan pengetahuan dan kesadaran.

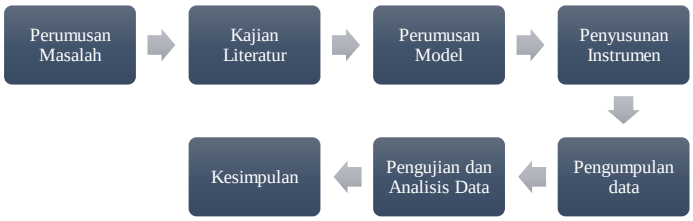
2) Penelitian Kedua

Penelitian yang dilakukan oleh Moti Zwilling et al. (2020) dengan judul "*Cyber Security Awareness, Knowledge and Behavior: A Comparative Study"* mereka melakukan analisis hubungan antara kesadaran *cyber security*, pengetahuan dan perilaku. Penelitian ini memiliki kekurangan yaitu belum melakukan uji validitas dan reliabilitas, sehingga peneliti perlu melakukan penelitian dengan melakukan uji validitas reliabilitas agar memberikan hasil yang maksimal.

III. METODOLOGI PENELITIAN

A. *Tahapan Penelitian*

Tahapan penelitian akan berisi metodologi penelitian yang dilakukan, berikut tahapan metodologi penelitian akan dijelaskan dibawah ini:



1) Perumusan masalah, pada tahapan ini merumuskan masalah yang akan digunakan dalam topik penelitian dalam hal ini faktor kesadaran dan pengetahuan *cyber security* pada pengguna *e-commerce* di Indonesia.

2) Kajian literatur yaitu melakukan kajian terhadap jurnal, artikel, atau buku yang berkaitan dengan topik penelitian

3) Perumusan model dan penyusunan instrumen adalah merumuskan model dari hasil analisis faktor, kemudian penyusunan instrumen yang merupakan kumpulan-kumpulan pertanyaan yang telah diberikan pilihan jawaban.

4) Pengumpulan data yaitu dengan menyebarkan kuisioner terhadap responden

5) Pengujian dan analisis data, melakukan pengujian validitas dan reliabilitas dengan teknik analisis *structural equation modeling* menggunakan program Rstudio.

6) Kesimpulan dilakukan setelah melakukan pengujian hipotesis dan mendapatkan hubungan antar variabel. Kesimpulan merupakan jawaban dari rumusan masalah penelitian.

B. Sampel dan Populasi

Populasi dari penelitian merupakan warga negara Indonesia, berusia minimal 13 tahun, dan pernah menggunakan segala bentuk *e-Commerce.* Dalam menggunakan teknik SEM disarankan penentuan jumlah sampel minimal yaitu 100 atau 200 sampel [11]. Memperhatikan jumlah pengguna *e-commerce* di Indonesia, standar probabilitas 95 persen, dan *margin of error* 5 persen, maka ditentukan jumlah sampel sebanyak 383 sehingga memenuhi jumlah sampel minimal dalam menggunakan teknik SEM.

C. Model, Konstruk, dan Indikator Penelitian

Penggunaan model pada Gambar 1 dalam penelitian ini berdasarkan hasil temuan dari analisis faktor yang menunjukkan bahwa pengetahuan dan kesadaran masing-masing memiliki 3 faktor yang dapat dijadikan sebagai endogen atau variabel dependen (DV) dalam analisis ini, yang kemudian membuat demografi menjadi eksogen atau variabel independen (IV). Sehingga hipotesis pada penelitian ini adalah:

1) H1: Kesadaran *cyber security e-commerce* memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

2) H2: Umur memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

3) H3: Jenis kelamin memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

4) H4: Pendidikan terakhir memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

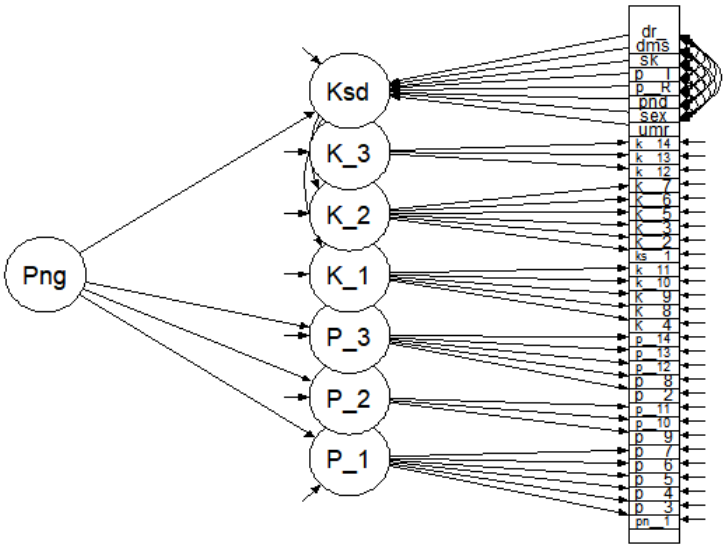
5) H5: Pendapatan rendah memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

6) H6: Pendapatan tinggi memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

7) H7: Sektor pekerjaan memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

8) H8: Domisili memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*

9) H9: Daerah asal memiliki hubungan signifikan terhadap pengetahuan *cyber security e-commerce*



Gambar 1 Diagram Jalur

Metode pengubahan data dari Gambar 1 yang akan diperlihatkan pada Tabel 1 tersebut nantinya bakal digunakan sebagai variabel penelitian, berikut bentuk peubah pada tabel 1:

Tabel 1 Metode Pengubah Data

	Variabel Laten	Variabel Indikator	Simbol
Eksogen	Demografi	Umur	Umr
		Jenis kelamin	Sex
		Pendidikan terakhir	pnd
		Pendapatan rendah	P_r
		Pendapatan tinggi	P_r
		Sektor pekerjaan	Sk_
		Domisili	Dms
		Daerah asal	Dsl_
Endogen	Pengetahuan Kejahatan (P_1)	Phising	P_1
		Carding	P_3
		Social Engineering	P_4
		Two FA	P_5
		Melindungi dari *Phising*, *cyber*crime, dan *social engineering*	P_6
		Situs *e-commerce* yang aman	P_7
	Pengetahuan Password (P_2)	*Password* yang kuat	P_9

		Password yang unik	P_10
		Menyimpan *password*	P_11
	Pengetahuan Transaksi (P_3)	*Cybercrime*	P_2
		Credit card bisa dicuri	P_8
		Kerentanan transaksi jaringan publik	P_12
		Tidak menyimpan data transaksi	P_13
		Tidak mengakses akun bank saat menggunakan jaringan publik	P_14
Endogen	Kesadaran Password dan Pencurian (K_1)	*Social Engineering*	K_4
		Credit card bisa dicuri	K_8
		Password yang kuat	K_9
		Password yang unik	K_10
		Menyimpan *password*	K_11
	Kesadaran Kejahatan (K_2)	*Phising*	K_1
		Cyber Crime	K_2
		Carding	K_3
		Two FA	K_5
		Melindungi dari *Phising, cybercrime, social engineering*	K_6
		Situs *e-commerce* yang aman	K_7
	Kesadaran Transaksi (K_3)	Kerentanan transaksi jaringan publik	K_12
		Tidak menyimpan data transaksi	K_13
		Tidak mengakses akun bank	K_14

Dari tabel kita bisa mengetahui bahwa masing-masing variabel memiliki tiga indikator, kecuali demografi. Kemudian, masing-masing indikator memiliki faktornya yang peneliti simbolkan dan peneliti gunakan sebagai pertanyaan kepada responden.

D. Pengumpulan Data

Untuk membantu dalam pengumpulan data, penelitian ini menggunakan metode kuisioner, dilakukan dengan cara membagikan kuisioner secara daring berdasarkan pertanyaan pada Tabel 1 berisikan jawaban yang telah ditentukan.

E. Data Responden

Setelah melakukan penyebaran kuisioner ke berbagai media sosial, maka terkumpul sebanyak 383 responden untuk dianalisis. Demografi dari responden adalah sebagai berikut:

1) Jenis Kelamin

Peneliti mendapatkan responden jenis kelamin laki-laki dengan persentase 40 persen dan jenis kelamin perempuan 60 persen.

2) Usia

Peneliti mendapatkan responden dengan rentang usia dari umur 15 tahun hingga 55 tahun.

3) Pendidikan Terakhir

Peneliti mendapatkan 68 persen responden pendidikan menengah (SMP dan SMA) dan 32 persen pendidikan tinggi (D-III, S1, S2, dan S3).

4) Pendapatan Bulanan

Peneliti mendapatkan 25 persen responden memiliki pendapatan kurang dari 1 Juta, 45 persen responden memiliki pendapatan 1 – 2,99 juta, sementara 13 persen responden memiliki pendapatan bulanan antara 3 – 4,9 juta, dan 17 persen memiliki pendapatan bulanan di atas 5 juta

5) Sektor Pekerjaan

Peneliti mendapatkan 55 persen responden tidak memiliki pekerjaan dan 45 persen memiliki pekerjaan.

6) Domisili dan Daerah Asal

Peneliti mendapatkan responden yang berdomisili di pulau Jawa dengan persentase 85 persen dan luar pulau Jawa 15 persen. Sementara daerah asal responden, mendapatkan sebanyak 63 persen berasal dari pulau Jawa dan 27 persen berasal dari luar pulau Jawa.

F. Pengujian Kuisioner

Untuk mengukur reliabel atau valid sebuah data terhadap indikator pada kuisioner yang akan digunakan terhadap penelitian ini, maka dilakukan pengujian validitas untuk mengukur valid sebuah data dan uji reliabilitas adalah menguji reliabel sebuah data.

G. Metode Analisis Data

Untuk menguji hasil hipotesis maka penelitian menggunakan teknik SEM (*Structural Equation Modeling)* dengan menggunakan R. *Structural Equation Modeling* merupakan teknik multivariat yang digunakan dengan menggabungkan analisis regresi (korelasi) dan analisis faktor untuk menguji dan mengevaluasi hubungan sebab akibat tiga atau lebih variabel laten dan konstruk [12].

IV. ANALISIS DAN HASIL

A. Analisis Data

Teknik statistik yang akan digunakan dalam uji penelitian ini yaitu teknik *structural equation modeling* (SEM) dengan pengujian validitas dan reliabilitas.

1) Uji Validitas dan Reliabilitas

Dilakukan uji validitas agar konsep penelitian benar-benar dapat diukur secara akurat, memberikan hasil data yang memiliki kaitan erat, dan menjalankan peran dari indikator seperti yang diinginkan [13]. Sementara uji reliabilitas merupakan berkaitan dengan seberapa konsisten alat ukur pada penelitian sehingga alat ukur tersebut dapat dipercaya dan dipergunakan [13].

Uji validitas penelitian ini menggunakan metode *bivariate pearson* yaitu melakukan perbandingan hasil *degree of freedom* (df) dan nilai pada r tabel. Indikator pada variabel dikatakan valid apabila nilai r tabel kurang dari nilai *degree of freedom* (df) yang bernilai positif [14]. Pada penelitian ini terdiri dari 383 responden dengan 28 variabel, sehingga r tabel untuk signifikansi 5% dengan n=383 adalah 0,098. Setelah dilakukan uji validitas, 28 indikator penelitian memiliki nilai diatas 0,098, sehingga data dapat dikatakan valid.

Untuk menguji reliabilitas data dilakukan dengan membandingkan nilai Cronbach Alpha 28 indikator penelitian dari 383 responden. Standar batas Cronbach Alpha untuk indikator yang akan digunakan penelitian ini yaitu 0,7. Setelah dilakukan pengujian, didapatkan hasil uji reliabilitas Cronbach Alpha dengan nilai sebesar 0,95. Sehingga keseluruhan data dalam penelitian ini reliabel dan valid, maka data dalam penelitian ini dapat dilanjutkan pada tahap analisis berikutnya.

2) Uji Goodness of Fit

Suatu model dapat diterima atau ditolak, maka kita harus menentukannya dengan melakukan analisis faktor konfirmatori (CFA) yaitu mengukur model *goodness of fit* antara variabel laten dengan indikator. Jika suatu model diterima maka selanjutnya kita menggunakan metode *Structural Equation Mode*ling (SEM) untuk melakukan interpretasi terhadap model yang telah diterima [15]. Hasil uji CFA pengetahuan dan pengetahuan dengan kesadaran dapat kita lihat pada Tabel 2 dan 3.

Tabel 2 Uji Goodness of Fit Pengetahuan

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0 [16]	2,52	Fit
SRMR	< 0,08 [17]	0,05	Fit
RMSEA	< 0,08 [18]	0,06	Fit
CFI	> 0,80 [17]	0,90	Fit
TLI	> 0,80 [19]	0,89	Fit

Berdasarkan Tabel 2, bisa dilihat masing-masing indikator sudah memenuhi standar dari para ahli yaitu ‘fit’ dan dapat dilakukan analisis nilai *estimate coefficient* pada uji *structural model*.

Tabel 3 Uji Goodness of Fit Pengetahuan dan Kesadaran

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0 [16]	3,51	Fit
SRMR	< 0,08 [17]	0,09	Acceptable fit
RMSEA	< 0,08 [18]	0,08	Fit
CFI	> 0,80 [17]	0,81	Marginal Fit
TLI	> 0,80 [19]	0,79	Marginal Fit

Berdasarkan Tabel 3, terdapat nilai marginal fit yang masih diterima untuk digunakan, karena hasil dari nilai *chi-square* dibagi dengan nilai *degree of freedom* (df) sebesar 3,51 yang menurut Wheaton et al. (1977) nilainya sudah berada di bawah angka 5 [16] dan merupakan ukuran yang dapat diterima untuk analisis selanjutnya.

Maka dapat disimpulkan bahwa model dari penelitian yang digunakan sekarang sudah dapat dikatakan ‘fit’ dan dapat menganalisis *estimate coefficient* pada uji *structural model* untuk langkah berikutnya. Menurut Chandio (2011), kata ‘fit’ bermaksud untuk menentukan seberapa baik model secara realistis memodelkan datanya.

3) Uji Structural Model

Parameter penilaian *estimate coefficient* merupakan hal yang krusial dalam hal melakukan uji *structural model* [20]. *Estimate coefficient* digunakan untuk melakukan evaluasi pemodelan hipotesis. Ketika pengujian probabilitas (p) memiliki nilai kurang dari ≤0,001 dan nilai dari *critical ratio* (C.R) mempunyai nilai lebih dari 1,96 maka pemodelan dapat dikatakan diterima dan dapat dilakukan interpretasi hasil. Tabel 4 dan 5 memperlihatkan hasil dari pengujian *structural model.*

Tabel 4 Structural Model Pengetahuan dan Demografi

Index	Estimate	C.R	P
Png > Umur	-0,001	-0,075	0,940
Png > Sex	0,438	4,690	0,000
Png > Pendidikan	0,103	0,906	0,365
Png > Pendapatan_bln_R	-0,128	-1,252	0,211
Png > Pendapatan_bln_T	0,006	0,027	0,978
Png > Sektor _job	0,089	0,875	0,382
Png > Domisili	-0,094	-0,678	0,498
Png > Daerah_asal	-0,154	1,518	0,129

Setelah dilakukan uji hipotesis pada tabel 4 kita bisa melihat, bahwa ada hubungan antara jenis kelamin dan pengetahuan *cyber security e-commerce* dinyatakan ada hubungan bersifat signifikan, karena nilai dari *critical ratio (C.R)* adalah 4,690,

kemudian *estimate* juga menghasilkan nilai sebesar 0,438, dan probabilitas (p) memiliki nilai kurang ≤0,001.

Tabel 5 Structural Model Pengetahuan dan Kesadaran

Index	Estimate	C.R	P
Ksd > Png	0,718	10,851	0,000
Ksd > Umur	-0,006	-1,160	0,246
Ksd > Sex	0,032	0,829	0,407
Ksd > Pendidikan	-0,028	-0,560	0,576
Ksd > Pendapatan_bln_R	-0,003	-0,073	0,941
Ksd > Pendapatan_bln_T	-0,167	-1,729	0,084
Ksd > Sektor _job	-0,018	-0,413	0,679
Ksd > Domisili	0,091	1,487	0,137
Ksd > Daerah_asal	0,042	-0,940	0,347

Berdasarkan hasil uji hipotesis pada Tabel 5 dapat diambil kesimpulan, kesadaran *cyber security* berpengaruh pada pengetahuannya terhadap *cyber security* dinyatakan terdapat hubungan signifikan, hal ini berdasarkan nilai *critical ratio (C.R)* sebesar 10,851, nilai *estimate* adalah 0,718, dan probabilitas (p) memiliki nilai ≤ 0,001

B. Hasil Hipotesis

Berdasarkan Tabel 4 dan 5 pemodelan dapat diterima dan cocok ketika nilai critical ratio (C.R) lebih dari 1,96 dan nilai probabilitas (P) kurang dari ≤0,001 mempunyai hubungan positif bersifat signifikan dan hipotesis dapat diterima. Berikut hasil hipotesis penelitian yang dapat diterima:

1) Hasil Hipotesis H1

Setelah dilakukan uji hipotesis, antara pengetahuan *cyber security e-commerce* (Png) dengan kesadaran *cyber security e-commerce* (Ksd) dinyatakan ada hubungan signifikan yang merupakan hipotesis pertama, hal ini dinyatakan dengan adanya hubungan positif yang signifikan, karena nilai dari *critical ratio (C.R)* adalah 4,690, kemudian *estimate* juga menghasilkan nilai sebesar 0,438, dan nilai probabilitas (p) kurang dari ≤0,001. hipotesis didukung dengan penelitian oleh Hyeun-Suk Rhee et al. (2009) dan kemudian peneliti coba perluas dalam konteks *cyber security*. Individu atau pelaku *e-commerce* dengan pengetahuan *cyber security* yang baik akan lebih sadar *cyber security*. Individu biasanya lebih mengetahui jenis kejahatan yang biasanya terjadi pada *e-commerce*. Selain itu, individu juga mampu mengetahui kriteria untuk jenis *password* yang kuat dan aman. Yang lebih menarik, individu mampu mengetahui dalam hal melindungi diri dari ancaman yang berkaitan dengan transaksi [21].

2) Hasil Hipotesis H3

Pada hasil uji hipotesis yang telah dilaksanakan, bahwa adanya hubungan antara pengetahuan *cyber security e-commerce* (Png) dan jenis kelamin dinyatakan dengan adanya hubungan yang signifikan yang merupakan hipotesis pertama, hal ini berdasarkan nilai *critical ratio (C.R)* sebesar 10,851, *estimate* yang memiliki nilai 0,718, dan nilai probabilitas (p) kurang dari ≤ 0,001. Hasil tersebut menunjukkan, jenis kelamin berpengaruh signifikan terhadap pengetahuan *cyber security*. Penelitian serupa juga menemukan bahwa perempuan merasakan tingkat risiko yang secara signifikan memiliki resiko lebih tinggi dalam belanja online [22]. Beberapa penelitian juga menunjukkan bahwa perbedaan jenis kelamin dalam penggunaan teknologi, perempuan telah terbukti memiliki tingkat masalah privasi yang lebih tinggi dalam penyebaran informasi mereka ketimbang laki-laki [23]. Oleh karena itu, hal ini mengungkapkan bahwa laki-laki memiliki perbedaan pengetahuan *cyber security* yang lebih tinggi dibandingkan perempuan

V. KESIMPULAN

Berdasarkan hasil analisis data, peneliti mendapatkan faktor-faktor yang mempengaruhi tingkat kesadaran *cyber security* yaitu pengetahuan *cyber security* memiliki hubungan positif yang berpengaruh signifikan terhadap kesadaran *cyber security*. Jika ancaman siber datang, maka individu dengan pengetahuan *cyber security* yang baik akan tersadar dengan ancaman dan akan segera mengamankan diri dari hal yang menggangu dalam menggunakan *e-commerce.*

Selain itu, perbedaan jenis kelamin merupakan salah satu faktor dalam hal pengetahuan *cyber security*. Penelitian ini mendapatkan hasil, bahwa terdapat kesenjangan pengetahuan yang besar antara laki-laki dan perempuan, di mana perempuan memiliki pengetahuan *cyber security* yang lebih rendah daripada laki-laki yang secara tidak langsung berpengaruh pada kesadaran *cyber security*. Sehingga hal ini membuat perempuan lebih rentan menjadi korban *cybercrime*. Sehingga temuan lain seperti data demografi, selain jenis kelamin ternyata tidak memiliki hubungan positif yang signifikan sehingga tidak dapat dijadikan acuan sebagai faktor penelitian.

Hal ke depan yang dapat dikerjakan dari penelitian ini adalah dengan menentukan konstruk penelitian yang lebih lanjut lagi dengan melakukan analisis perbandingan antara kesadaran penjual dan kesadaran pembeli *e-commerce,* karena penelitian ini hanya mencakup pengguna secara keseluruhan, belum melakukan analisis antara penjual dan pembeli.

VI. REFERENSI

[1] K. Das, T. Tamhane, B. Vatterott, P. Wibowo dan S. Wintels, “The digital archipelago: How online commerce is driving Indonesia’s economic development,” *McKinsey & Company,* pp. 1-72, 2018.

[2] GlobalWebIndex, “Commerce Flagship Report on the Latest Trends in Online Commerce,” 2019.

[3] Statista, “eCommerce,” Statista, May 2020. [Online]. Available: https://www.statista.com/outlook/243/120/ecommerce/indonesia#market-users.

[4] U. Amaliya, “E-Commerce di Singapura dan Indonesia : Sebuah Perbandingan Kebijakan,” *Jurnal*

Ilmu Sosial dan Ilmu Politik, vol. 1, no. e-commerce, pp. 1-21, 2009.

[5] M. Bishop, "What is computer security?," *IEEE Security & Privacy,* vol. 1, no. 1, pp. 67-69, 2003.

[6] Direktorat Tindak Pidana Siber Bareskrim Polri, "Patroli Siber," Desember 2019. [Online]. Available: https://patrolisiber.id/statistic.

[7] V. Zwass, "Electronic Commerce: Structures and Issues," *International Journal of Electronic Commerce,* vol. 1, no. 1, pp. 3-23, 1996.

[8] AO Kaspersky Lab, "What is Cyber Security?," AO Kaspersky Lab, 2019. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Diakses Juni 2020].

[9] R. S. Shaw, C. C. Chen, A. L. Harris dan H.-J. Huang, "The impact of information richness on information security awareness," *Computers & Education,* vol. 52, pp. 92-100, 2009.

[10] J. B. Ullman dan P. M. Bentler, "Structural Equation Modeling," *Handbook of Psychology,* 2003.

[11] E. J. Wolf, K. M. Harrington, S. L. Clark dan M. W. Miller, "Sample Size Requirements for Structural Equation Models: An Evaluation of Power, Bias, and Solution Propriety," *Educational and Psychological Measurement,* vol. 73, no. 6, pp. 913-934, 2013.

[12] J. Hox dan T. Bechger, "An Introduction to Structural Equation Modeling," *Family Science Review,* vol. 11, pp. 354-373, 1999.

[13] R. Heale dan T. Alison, "Validity and reliability in quantitative studies," *Evidence-Based Nursing,* vol. 18, no. 3, pp. 66-67, 2015.

[14] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Bandung: Alfabeta, 2009.

[15] P. F. Holgado-Tello, S. Chacon-Moscoso, I. Barbero-Garcia dan E. Vila-Abad, "Polychoric versus Pearson correlations in exploratory," *Quality and Quantity,* pp. 153-166, 2010.

[16] B. Wheaton, B. Muthen, D. F. Alwin dan G. F. Summers, "Assesing Reliability and Stability in Panel Models," *Sociological Methodology,* vol. 8, pp. 84-136, 1977.

[17] L.-t. Hu dan P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives.," *Structural Equation Modeling,* pp. 1-55, 1999.

[18] R. C. MacCallum, M. W. Browne dan H. M. Sugawara, "Power Analysis and Determination of Sample Size for," *Psychological Methods,* vol. 1, no. 2, pp. 130-149, 1996.

[19] H. W. Marsh, J. R. Balla dan R. P. McDonald, "Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size.," *Psychological Bulletin,* vol. 103, no. 3, pp. 391-410, 1988.

[20] F. H. Chandio, "Studying acceptance of online banking information system: A structural equation model," *Brunel University Brunel Business School PhD Theses,* 2011.

[21] H.-S. Rhee, C. Kim dan Y. U. Ryu, "Self-efficacy in information security: Its influence on end," *Computers & Security ,* vol. 28, pp. 816-826, 2009.

[22] E. Garbarino dan M. Strahilevitz, "Gender differences in the perceived risk of buying online and the," *Journal of Business Research,* vol. 57, pp. 768-775, 2004.

[23] S. Chai, S. Das dan H. R. Rao, "Factors Affecting Bloggers' Knowledge Sharing: An Investigation Across Gender," *Journal of Management Information Systems,* vol. 28, pp. 309-342, 2014.