Analisis Kesadaran Cyber Security Pada Kalangan Pelaku e-Commerce di Indonesia

by John Doe

Submission date: 02-Jun-2020 02:44PM (UTC+0700)
Submission ID: 1334633417
File name: Makalah_TA_Kolokium.pdf (636.29K)
Word count: 3079
Character count: 18670

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

***Abstrak*—Hadirnya *e-commerce* di Indonesia sebagai aktivitas pembelian atau penjualan barang atau jasa melalui internet memungkinkan dapat terjadinya kejahatan siber atau biasa disebut *cyber crime*. Ancaman terjadinya *cyber crime* merupakan hal yang dapat mengganggu aktivitas *e-commerce* sehingga, konsumen maupun pelaku usaha harus mampu melindungi dari ancaman tersebut dengan *cyber security*. Dengan begitu, peneliti berusaha mencoba meneliti bagaimana tingkat kesadaran dari para pelaku *e-Commerce* terhadap ancaman *cyber crime*. Analisis data ini menggunakan sumber data primer dari hasil kuisioner yang dibagikan kepada pengguna *e-Commerce*. Untuk mengukur hubungan antar variabel laten berupa Kesadaran dan Pengetahuan *Cyber Security* dengan Demografi pengguna *e-Commerce* menggunakan Teknik *Structural Equation Modeling* (SEM). 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*..**

Keywords—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. Dengan 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, menginkatkan akses yang tanpa batas, dan konektivitas dengan skala yang lebih besar dalam lokal maupun skala global [1].

Menurut data GlobalWebIndex, 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].

Hadirnya *e-commerce* di Indonesia sebagai aktivitas pembelian atau penjualan produk melalui internet memberikan pengguna dapat berkomunikasi dengan menyamarkan identitasnya, tanpa dibatasi oleh batas wilayah, dan bahkan lintas negara sehingga dapat memungkinkan dapat terjadinya kejahatan siber atau biasa disebut *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 kejahatan siber atau *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 *cyber crime* 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 kejahatan siber 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.

Risiko keaman 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 memliki kekurangan yaitu sampel yang digunakan untuk survei seluruhnya terdiri dari mahasiswa sarjana dalam kursus lanjutan dari satu universitas dan mereka tidak mewakili populasi *e-Commerce* keseluruhan.

Berangkat dari segala permasalahan dan kejahatan yang terjadi pada *e-Commerce* peneliti mencari tahu faktor-faktor yang mempengaruhi tingkat kesadaran dan pengetahuan *cyber security* pada kalangan pelaku *e-Commerce* di Indonesia.

II. METODOLOGI PENELITIAN

Bab ini akan berisi bagaimana metodologi penelitian yang dilakukan pada penelitian ini, berikut metodologi penelitian yang akan dijelaskan pada subbab dibawah ini:

A. Sampel dan Populasi

Dalam menentukan populasi, pengambilan sampel dilakukan secara acak. Populasi dari penelitian merupakan warga negara Indonesia berusia minimal 13 tahun yang pernah menggunakan *e-Commerce*. Dalam menggunakan teknik SEM disarankan penentuan jumlah sampel minimal yaitu 100 atau 200 sampel [7]. Pada penelitian ini Menggunakan 383 sampel sehingga telah memenuhi kriteria tersebut.

B. Metode Pengumpulan Data

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

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 (DV) dalam analisis ini, yang kemudian membuat demografi menjadi Eksogen (IV). Dengan 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

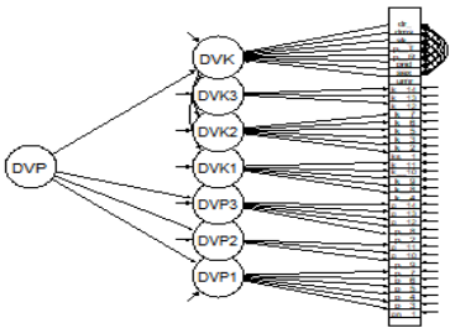
5) H5: Pendapatan rendah memiliki hubungan signifikan terhadap Pengetahuan cyber security e-Commerce

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 Path Diagram

Berikut metode pengubahan data yang akan digunakan pada Tabel 1:

Table 1 Metode Pengubah Data

	Konstruk/Peubah *Latent*	Indikator/Peubah *Manifest*	Peubah
Eksogen	Demografi	Umur	Umr
		Sex	Sex
		Pendidikan Terakhir	pnd
		Pendapatan Rendah	P_r
		Pendapatan Tinggi	P_r
		Sektor Pekerjaan	Sk_
		Domisili	Dms
		Daerah Asal	Dsl_
Endogen	Kejahatan (DVP1)	Phising	P_1
		Carding	P_3
		Social Engineering	P_4
		Two FA	P_5
		Melindungi dari Phising, cyber, social	P_6
		Situs e-commerce yang aman	P_7
	Password (DVP2)	Password yang kuat	P_9
		Password yang unik	P_10
		Menyimpan password	P_11
	Transaksi (DVP3)	Cyber Crime	P_2
		Credit card bisa di curi	P_8
		Kerentanan transaksi jaringan public	P_12
		Tidak menyimpan data tramsaksi	P_13
		Tidak mengaksi akun bank	P_14

Eksogen	Password dan Pencurian (DVK1)	Social Engineering	K_4
		Credit card bisa di curi	K_8
		Password yang kuat	K_9
		Password yang unik	K_10
		Menyimpan password	K_11
	Kejahatan (DVK2)	Phising	K_1
		Cyber Crime	K_2
		Carding	K_3
		Two FA	K_5
		Melindungi dari Phising, cyber, social	K_6
		Situs e-commerce yang aman	K_7
	Transaksi (DVK3)	Kerentanan transaksi jaringan publik	K_12
		Tidak menyimpan data transaksi	K_13
		Tidak mengakses akun bank	K_14

D. Data Responden

Penelitian ini memfokuskan populasi pada warga Indonesia yang berusia minimal 13 tahun dan pernah menggunakan *e-Commerce*. Dari penyebaran ke berbagai media sosial maka, terkumpul sebanyak 383 responden untuk dianalisis. Ada pun demografi dari responden sebagai berikut:

1) Jenis Kelamin

Dari seluruh responden, mendapatkan untuk jenis kelamin laki-laki berjumlah 40 persen dan jenis kelamin perempuan berjumlah 60 persen.

2) Usia

Dari seluruh responden rentang usia yang didapatkan dari pengumpulan yaitu dari umur 15 tahun hingga 55 tahun.

3) Pendidikan Terakhir

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

4) Pendapatan Bulanan

Dari seluruh responden peneliti mendapatkan 25 persen memiliki pendapatan kurang dari 1 Juta, 45 persen memiliki pendapatan 1 – 2,99 juta, sementara 13 persen responden memiliki pendapatan bulanan antara 3 – 4,9 juta, dan 17 persen memiliki pendapatan bulanan diatas 5 juta

5) Sektor Pekerjaan

Dari seluruh responden peneliti mendapatkan 55 persen responden tidak memiliki pekerjaan dan 45 persen memiliki pekerjaan.

6) Domisili dan Daerah Asal

Dari seluruh responden didapatkan bahwa untuk yang berdomisili di pulau Jawa peneliti mendapatkan responden berjumlah 85 persen dan luar pulau Jawa berjumlah 15 persen. Sementara daerah asal responden, mendapatkan sebanyak 63 persen berasal dari pulau Jawa dan 27 persen berasal dari luar pulau Jawa.

E. Pengujian Kuisioner

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

F. Metode Analisis Data

Untuk menguji hasil hipotesis maka penelitia 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 [8].

III. 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 [9]. Sementara uji reliabilitas merupakan berkaitan dengan seberapa konsisten alat ukur pada penelitian sehingga alat ukur tersebut dapat dipercaya dan dipergunakan [9].

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 [10]. 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.

Membandingkan nilai Cronbach Alpha untuk menguji reliabilitas data dilakukan dengan 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 reliabilitas Cronbach Alpha dengan memperoleh nilai sebesar 0,95. Dikarenakan keseluruhan data dalam penelitian ini reliabel dan valid maka, data dalam penelitian ini dapat dilanjutkan pada tahap analisis.

2) Uji Goodness of Fit

Suatu model dapat diterima atau ditolak, maka kita harus menentukannya dengan analisis faktor konfirmatori (CFA) yaitu untuk mengukur model *goodness of fit* antara variabel laten dengan indikator. Jika suatu model diterima maka selanjutnya kita menggunakan metode *Structural Equation Modeling* (SEM) untuk melakukan interpretasi terhadap model yang telah diterima [11]. Hasil uji CFA pengetahuan dan pengetahuan dengan kesadaran dapat kita lihat pada Tabel 2 dan 3.

Table 2 Uji Goodness of Fit Pengetahuan

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0 [12]	2,52	Fit
SRMR	< 0,08 [13]	0,05	Fit
RMSEA	< 0,08 [14]	0,06	Fit
CFI	> 0,80 [13]	0,90	Fit
TLI	> 0,80 [15]	0,89	Fit

Table 3 Uji Goodness of Fit Pengetahuan dan Kesadaran

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0 [12]	3,51	Fit
SRMR	< 0,08 [13]	0,09	Acceptable fit
RMSEA	< 0,08 [14]	0,08	Fit
CFI	> 0,80 [13]	0,81	Marginal Fit
TLI	> 0,80 [15]	0,79	Marginal Fit

Berdasarkan Tabel 2 dan 3 model dari penelitian yang digunakan sekarang sudah dapat dikatakan 'fit'. 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* [16]. *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*.

Table 4 Structural Model Pengetahuan dan Demografi

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

Table 5 Structural Model Pengetahuan dan Kesadaran

Index	Estimate	C.R	P
DVK > DVP	0,718	10,851	0,000
DVK > Umur	-0,006	-1,160	0,246
DVK > Sex	0,032	0,829	0,407
DVK > Pendidikan	-0,028	-0,560	0,576
DVK > Pendapatan_bln_R	-0,003	-0,073	0,941
DVK > Pendapatan_bln_T	-0,167	-1,729	0,084
DVK > Sektor _job	-0,018	-0,413	0,679
DVK > Domisili	0,091	1,487	0,137
DVK > 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* (DVP) dengan Kesadaran *cyber security e-Commerce* (DVK) 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 [17].

2) Hasil Hipotesis H3

Pada hasil uji hipotesis yang telah dilaksanakan, bahwa adanya hubungan antara Pengetahuan *cyber security e-Commerce* (DVP) 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 [18]. 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 [19]. Oleh karena itu, hal ini mengungkapkan bahwa laki-laki memiliki kesenjangan pengetahuan *cyber security* yang lebih tinggi dibandingkan perempuan

IV. KESIMPULAN

Berdasarkan hasil analisis data, Pengetahuan *Cyber Security* memiliki hubungan positif yang memiliki pengaruh signifikan terhadap Kesadaran *Cyber Security*. Ketika ancaman datang, individu dengan Pengetahuan *cyber security* yang baik mereka akan tersadar dan akan segera mengamankan diri dari hal yang dirasa dapat menggangu dalam menggunakan *e-Commerce*.

Selain itu, peneliti mendapatkan temuan menarik bahwa Jenis kelamin merupakan faktor penting dalam *cyber security*. Dalam hal Pengetahuan *cyber security,* penelitian ini mendapatkan hasil bahwa terdapat kesenjangan pengetahuan yang besar antara laki-laki dan perempuan mana perempuan yang memiliki pengetahuan *cyber security* lebih rendah daripada laki-laki yang secara tidak langsung berpengaruh pada kesadaran *cyber security*. Sehingga hal ini membuat perempuan lebih rentan menjadi korban *cybercrime*.

Hal ke depan yang dapat dikerjakan dari penelitian ini yaitu dengan menentukan konstruk penelitian yang paten dan saling berkaitan sehingga dapat meningkat tingkat presisi yang lebih tinggi dalam analisis.

V. 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," 2018.

[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] 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.

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

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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

Analisis Kesadaran Cyber Security Pada Kalangan Pelaku e-Commerce di Indonesia

ORIGINALITY REPORT

18%	14%	11%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ndltd.ncl.edu.tw Internet Source	2%
2	fedetd.mis.nsysu.edu.tw Internet Source	1%
3	www.hindawi.com Internet Source	1%
4	Submitted to Universitas Negeri Jakarta Student Paper	1%
5	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	1%
6	Submitted to Universitas Brawijaya Student Paper	1%
7	45073f2c-fc7c-4774-b547-a5ea92c2e28c.filesusr.com Internet Source	1%
8	Submitted to Universiti Teknologi Petronas Student Paper	1%

9	www.audiologyresearch.org Internet Source	1%
10	repository.its.ac.id Internet Source	1%
11	Submitted to University of Hull Student Paper	1%
12	Field, C.A.. "Construct, concurrent and predictive validity of the URICA: Data from two multi-site clinical trials", Drug and Alcohol Dependence, 20090401 Publication	1%
13	www.computer.org Internet Source	1%
14	citeseerx.ist.psu.edu Internet Source	1%
15	Submitted to Australian National University Student Paper	1%
16	jthmnet.com Internet Source	1%
17	Submitted to Padjadjaran University Student Paper	1%
18	Submitted to Binus University International Student Paper	1%
19	ejournal.poltektegal.ac.id	

	Internet Source	<1%
20	Submitted to University of Warwick Student Paper	<1%
21	bura.brunel.ac.uk Internet Source	<1%
22	eprints.uny.ac.id Internet Source	<1%
23	issuu.com Internet Source	<1%
24	Qurrotul Ainiyah. "Poligami di Indonesia dalam perspektif CEDAW dan mazhab Shafi'i", Ijtihad : Jurnal Wacana Hukum Islam dan Kemanusiaan, 2017 Publication	<1%
25	www.tandfonline.com Internet Source	<1%
26	Jürgen Bortz, Nicola Döring. "Forschungsmethoden und Evaluation", Springer Science and Business Media LLC, 2006 Publication	<1%
27	scholarscompass.vcu.edu Internet Source	<1%
	Submitted to Atma Jaya Catholic University of	

28	Indonesia Student Paper	<1%
29	Submitted to iGroup Student Paper	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

Analisis Kesadaran Cyber Security Pada Kalangan Pelaku e-Commerce di Indonesia