Versi Online: http://journal.ubm.ac.id/
Hasil Penelitian

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

PENGARUH *CYBER CRIME* TERHADAP *CYBER SECURITY COMPLIANCE* DI SEKTOR KEUANGAN

Febrian Kwarto [1] , Madya Angsito [2]
Universitas Mercu Buana
febrian_kwarto@mercubuana.ac.id [1] , madya.angsito@gmail.com [2]

ABSTRACT: *The main purpose of this study to have evidence empirically the effect of Cyber Crime on Cyber Security Compliance in Financial Sector. Independent variables used in this study are hacking, phishing, malware. While the dependent variable in this study is the cyber security compliance in financial sector. This study uses a survey on the Bank Office in Jakarta area which are the respondents on this study are IT Staff. Data collected by spreading questionnaire with convenience sampling method. There are 367 questionnaires distributed, 367 back, and the 367 questionnaires that could be analyzed. Data processing is performed by using descriptive statistical tests, validity, reliability test, classic assumption test, test the coefficient of determination, test multiple linear regression analysis and hypothesis testing with the help of Statistical Product and Service Solution (SPSS) version 21 and Microsoft Excel 2013. The results of this processing indicates that hacking empirically affect on cyber security compliance in financial sector, phising empirically affect the cyber security compliance in financial sector, and malware empirically affect the cyber security compliance in financial sector*.

Keyword *: Hacking, Phising, Malware, Cyber, Financial Sector*

ABSTRAK: Penelitian ini bertujuan untuk membuktikan secara empiris pengaruh *Cyber Crime* terhadap *Cyber Security Compliance* di Sektor Keuangan. Variabel independen yang digunakan dalam penelitian ini adalah *hacking, phising* dan *malware.* Sedangkan variabel dependen dalam penelitian ini adalah *cyber security compliance* di sektor keuangan. Penelitian ini menggunakan metode *survey* pada kantor perbankan yang berada di Jakarta dengan responden yang dituju adalah staf IT. Data dikumpulkan dengan menyebar kuesioner dengan metode *convenience sampling.* Terdapat 367 kuesioner yang disebarkan, 367 kembali, dan 367 kuesioner yang dapat dianalisis. Pengolahan data dilakukan dengan menggunakan uji statistic deskriptif, uji validitas, uji reliabilitas, uji asumsi klasik, uji koefisien determinasi, uji analisis regresi linear berganda dan uji hipotesis dengan bantuan *Statistical Product and Service Solution* (SPSS) versi 21 dan Microsoft Excel 2013. Hasil penelitian ini menunjukan bahwa *hacking* secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan, *phising* secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan, dan *malware* secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan.

Kata kunci: *Hacking, Phising, Malware,* Siber, Sektor Keuangan

I. Pendahuluan

1.1. Latar Belakang

Teknologi yang semakin berkembang saat ini yang seiring dengan kebutuhan manusia akan tekhnologi tersebut mengakibatkan berbagai inovasi dan penemuan baru yang juga semakin berkembang. Hal ini dapat dilihat dari banyaknya penemuan-penemuan berbasis teknologi *(gadget)* seperti *smartphone*, *laptop*, televisi, *air conditioner*, *personal computer* (PC), gelombang radio, dsb. Namun dibalik semakin maju dan berkembangnya teknologi ini, teknologi tidak hanya memberikan dampak positif bagi masyarakat melainkan juga dampak negatif yang tidak luput dari pemanfaatan teknologi itu sendiri.

Salah satu bentuk nyata dari dampak negatif teknologi itu sendiri adalah *Cybercrime. Cybercrime* atau dalam bahasa Indonesia disebut dengan kejahatan dunia maya adalah pelanggaran yang hanya dapat dilakukan menggunakan komputer, jaringan komputer atau bentuk lain dari teknologi komunikasi informasi (McGuire, Mike, and Samantha Dowling, 2013). Tindakan ini

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

meliputi penyebaran virus atau *malware* lainnya, pembajakan *(hacking),* dan penolakan-penolakan yang dikirim melalui serangan pada layanan yang terdapat dalam *software*. Mereka adalah kegiatan yang diarahkan untuk menyerang sistem terutama terhadap komputer atau sumber daya jaringan. Misalnya, data yang dikumpulkan/didapatkan dengan cara menyusup ke dalam akun *e-mail* dapat digunakan sebagai alat untuk melakukan penipuan.

Kasus *cybercrime*, baik korban maupun pelaku tidak berhadapan langsung dalam 1 (satu) tempat dimana kejadian perkara terjadi, bahkan dapat terjadi antar negara. Hal ini membuktikan bahwa *cybercrime* merupakan salah satu bentuk kejahatan lintas negara *(transnational crime),* tanpa batas *(borderless),* tanpa kekerasan *(non violence),* tidak ada kontak fisik (*non phisically contact*) dan tiada nama *(anonimity)* (Balian Zahab, 2010).

Tujuan utama dari *cybercrime* sendiri adalah untuk mendapatkan keuntungan pribadi bagi si pelaku dengan cara yang ilegal. Hal ini dikarenakan *cybercrime* merupakan tindak kejahatan yang serius yang telah diatur dalam Undang-Undang mengenai dampak yang diberikan beserta sanksinya. Kemudian, tujuan *cybercrime* untuk meraup keuntungan materi dapat dilihat dari banyaknya kasus yang menimpa sejumlah sektor di pemerintahan khususnya sektor keuangan yang sarat akan hal-hal yang bersifat material. Sektor keuangan memang merupakan suatu wadah yang sangat menggiurkan bagi para pelaku cybercrime untuk melakukan tindak kejahatan mereka, karena semua yang bersifat material diatur dalam sektor tersebut.

1.2. Identifikasi Masalah

Dalam beberapa tahun terakhir setidaknya terdapat 3 jenis *cybercrime* yang seringkali menyerang sektor keuangan di Indonesia, diantaranya *hacking, phising dan malware*. Ketiga *cybercrime* ini tidak hanya menyerang sektor keuangan melainkan juga sektor lain yang memungkinkan untuk diretas atau disusupi. Hal ini mengindikasikan bahwa indonesia merupakan termasuk salah satu negara yang lemah *cyber security*nya

Seperti kasus yang baru-baru ini terjadi yang menyerang sektor publik di bidang kesehatan, yang sebenarnya tetap bermuara kepada tebusan uang, dua rumah sakit di Jakarta terjangkit program jahat jenis *ransomware* bernama *WannaCry*.
Malware bermodus menyandera data dan meminta tebusan uang itu telah mengunci sistem dan data pasien di RS Dharmais dan RS Harapan Kita. Pembuat *WannaCry* meminta uang Rp 4 juta sebagai tebusan. Hal serupa juga terjadi di Rumah sakit di Hollywood Presbyterian *Medical Center* di Los Angeles, Amerika Serikat (AS). Pihak rumah sakit harus rela merogoh kantongnya untuk mengeluarkan uang hingga 17.000 dollar atau sekitar Rp 226 juta demi menebus data yang disandera penyerang. Menurut administrator rumah sakit Harapan Kita Jakarta untuk bahwa solusi untuk mendapatkan kembali akses yang terputus itu adalah dengan membayar sejumlah uang pada penyerangnya. (Kompas Tekno, 14 Mei 2017).
Sementara itu, berdasarkan informasi yang didapatkan (Metro TV news, 10 Mei 2017) sektor keuangan dan pemerintahan masih menjadi incaran utama para *hacker*. Riset terbaru mengungkapkan bahwa serangan siber pada sektor pemerintahan berlipat ganda di tahun 2016, meningkat menjadi 14 % dari 7 % untuk semua ancaman keamanan siber di 2015. Serangan yang terjadi pada sektor keuangan juga meningkat secara pesat dari hanya 3 % di 2015 menjadi 14 % untuk semua serangan di 2016. Dengan mendapatkan akses pada aset digital dan data pelanggan tersebut memungkinkan para pelaku kejahatan siber untuk mendapatkan keuntungan dari informasi pribadi dan data kartu kredit. Hal menarik lainnya adalah 63 % dari semua ancaman siber berasal dari alamat IP di Amerika Serikat, diikuti oleh Inggris (4 %), dan Tiongkok (3 %). Selain itu, ancaman siber kini juga telah merambah ke perangkat IoT. Dari serangan IoT yang terdeteksi pada tahun 2016, sekitar 66 %

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

mencoba menemukan perangkat tertentu seperti model kamera video tertentu, 3 % mencari *server web* atau jenis *server* lainnya, sementara 2 % mencoba menyerang *database*.

Tabel 1
Perkiraan Kerugian akibat *Cyber Crime*

	Global	Indonesia
GDP	USD 71,620 bn	USD 895 bn
Percent of global GDP		
Cost of		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cyber crime	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Sumber: Meeting the cyber-security challenge in Indonesia. An analysis of threats and responses A report from DAKA advisory, hal 22

Tabel ini mendeskripsikan bahwa perkiraan resiko akibat Cyber Crime di Indonesia dapat terkomparasi dengan perkiaan kerugian global yang terjadi di dunia, perkiraan ini menjadikan Indonesia menurut data CIA diatas telah mencapai 1,20 % dari tingkat kerugian akibat cyber crime yang terjadi di dunia

Kasus-kasus diatas tentunya menunjukkan suatu fenomena bahwasannya bagaimana bisa suatu sistem informasi yang dimiliki oleh suatu organisasi/instansi/lembaga *elite* diretas dan diinfeksi oleh orang-orang yang identitas dan keberadaannya tidak diketahui. Sistem informasi milik organisasi/instansi/lembaga *elite* sudah pasti dikelola oleh para tenaga ahli yang profesional dibidangnya masing-masing. Namun secara empiris sistem tersebut masih dapat dimasuki dan bahkan dirusak secara permanen oleh para pelaku kejahatan tersebut *(hacker).* Hal ini tentunya menimbulkan spekulasi apakah organisasi/instansi/lembaga elit yang berada di Indonesia telah menerapkan *cyber security compliance* dengan baik dan benar.

1.3. Tujuan dan Manfaat Penelitian

Tujuan penelitian ini adalah untuk melihat apakah *cybercrime* yang terdiri atas *hacking*, *phising* dan *malware* berpengaruh terhadap *cybersecurity compliance* di sektor keuangan? Dengan kata lain apakah jika pelaku *Cyber* mematuhi aturan aturan keamanan dan etika yang berlaku dalam dunia maya akan dapat terhindar dari beberapa kejahatan siber?

Selain itu tujuan dari penelitan ini juga untuk menganalisis dan mengetahui seberapa besar pengaruh *hacking, phising* dan *malware* terhadap *cybersecurity compliance* di sektor keuangan. Sehingga dapat dijadikan pedoman bagi pihak perbankan ataupun industri lainnya yang juga akan mempengaruhi sektor keuangannya dalam meningkatkan keamanan sistem jaringan agar tidak mudah diretas dan dibajak oleh para pelaku *cybercrime.*

II. Kajian Pustaka

2.1. *Cybersecurity Compliance* di Sektor Keuangan

Cyber security perlindungan terhadap komputer dan seluruh informasi yang terdapat pada komputer, karena tanpa cyber Security semua data yang terdapat pada komputer akan dapat terhapus atau dicuri. (Haq,Kamar 2018, p 8) Kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Ronald (Thompson & William Cats Barril, 2003,p.29), (Handrini, 2014) Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil,

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

Cyber Security Compliance merupakan upaya evaluasi yang dilakukan untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan cyber. Tujuan dari upaya ini adalah untuk memastikan dan mengamati apakah organisasi/instansi/lembaga yang ada di Indonesia telah menjalankan tanggung jawab mereka dengan bijak dan cermat dalam memproteksi keamanan sistem informasi yang dimiliki dari berbagai ancaman siber yang ada di sekitar.

2.2. *Cybercrime*

Pada masa awalnya, cyber crime didefinisikan sebagai kejahatan komputer (computer crime). *The British Law Commission*, mengartikan "*computer crime*" sebagai manipulasi komputer dengan cara apa pun yang dilakukan dengan iktikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandell membagi "*computer crime*" atas dua kegiatan, yaitu:

a. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keunangan, keuntungan bisnis, kekayaan atau pelayanan.
b. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cyber crime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen *hardware*-nya saja kejahatan itu dimaknai sebagai *cyber crime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan. sehingga lebih tepat jika pemaknaan dari *cyber crime* adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara (Arryaguna, 2017).

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem informasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

2.3. Pengembangan Hipotesis

Hacking

Menurut Khairul Anam (2010) *hacking* merupakan kegiatan mengakses atau menyusup ke sistem komputer dan sistem elektronik tanpa hak. *Hacking* sebagai sebuah bentuk kegiatan kejahatan telah ada dan berkembang bersama perkembangan teknologi komputer dan internet. Seseorang yang memiliki keahlian lebih dalam penguasaan komputer baik dari sistem, *software* ataupun *hardware* dan memiliki keinginan untuk dapat memasuki dan merusak sistem komputer sendiri dinamakan dengan sebutan *hacker.*

Memasuki dalam arti masuk ke sistem pertahanan atau sistem keamanan suatu data yang dimiliki oleh orang lain (membobol) untuk mengambil data atau sesuatu yang dibutuhkan oleh *hacker.* Sedangkan merusak dapat diartikan merusak data atau menghilangkan data bahkan bisa memberikan *virus* pada sistem pertahanan yang dimiliki oleh orang tersebut setelah masuk ke dalam sistem komputer tersebut atau setelah mengambil sesuatu yang dibutuhkannya (Sitorus 2004 dalam Adi Pusdyanto, 2008).

H1: *Hacking* berpengaruh positif terhadap *cyber security compliance* di sektor keuangan.

Phising

Phising merupakan kegiatan memancing pemakai komputer di internet *(user)* agar mau memberikan informasi data diri

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

pemakai *(username)* dan kata sandinya *(password)* pada suatu *website* yang sudah di-*deface*. *Phising* biasanya diarahkan kepada pengguna *online banking.* Isian data pemakai dan *password* yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya. *Phising* biasanya dilakukan melalui *e-mail spoofing* atau pesan instan, dan sering mengarahkan pengguna untuk memasukkan rincian di sebuah *website* palsu yang tampilan dan nuansa yang hampir sama dengan yang aslinya (Ketaren, 2016).

H2: *Phising* berpengaruh positif terhadap *cyber security compliance* di sektor keuangan.

Malware

Merupakan program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau *operating system. Malware* terdiri dari berbagai macam, yaitu: virus, *worm, trojan horse, adware, browser hijacker*, dll. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisipkannya di sebuah aplikasi ataupun file tertentu (Ketaren, 2016).

Menurut Adenansi dan Novarina (2017) Malware dapat menyebar dengan cepat di jaringan tanpa campur tangan dari pengguna. Sistem pendektesian malware masih menjadi masalah karena varian malware baru yang selalu berkembang dengan menggunakan teknik yang berbeda untuk menghindari metode pendeteksian.

Sasaran utama dari *malware* adalah untuk memata-matai seseorang, mencuri informasi atau data pribadi (rahasia) orang lain seperti *m-banking*, membobol *security program* (program keamanan) dan lain-lain.

H3: *Malware* berpengaruh positif terhadap *cyber security compliance* di sektor keuangan.

III. Metode Penelitian

3. 1 Ruang Lingkup Penelitian

Penelitian ini bertujuan untuk menganalisa pengaruh *hacking*, *phising* dan *malware* terhadap *cybersecurity compliance* di sektor keuangan. Jenis dan sumber data yang dipakai dalam penelitian ini adalah data primer yang di peroleh langsung dari hasil pengisian kuisioner yang peneliti sebarkan. Populasi yang digunakan dalam penelitian ini adalah kantor perbankan yang berada di wilayah DKI Jakarta. DKI Jakarta dipilih dalam penelitian ini karena merupakan pusat dari seluruh kegiatan pemerintahan termasuk sektor keuangan khususnya.

3. 2 Metode Penentuan Sampel

Untuk menentukan sampel yang akan digunakan dalam penelitian, peneliti menggunakan teknik pengambilan sampel dengan *convenience sampling*. Hal ini disebabkan karena kurangnya akses untuk mencari responden yang sesuai dengan kriteria penelitian ini. Yang menjadi sampel dalam penelitian ini yaitu staf IT kantor perbankan di DKI Jakarta, Alasan mengambil sampel penelitian staf IT kantor perbankan untuk menjadi responden kuisioner dalam penelitian ini, dikarenakan pihak staf IT yang memiliki kemampuan komputerisasi yang handal serta memiliki kemampuan serta pengetahuan dalam membangun sistem keamanan (proteksi) untuk kantor perbankan. Selain itu, staf IT memiliki wewenang untuk mengusulkan perbaikan (*maintenance*) dan pembaharuan (*upgrade*) kepada atasan di kantor perbankan tersebut. Sementara perbankan yang menjadi objek penelitian ini dikarenakan dunia perbankan sangat erat hubungannya dengan sektor keuangan, sehingga berbagai analisa dan resiko rugi yang akan terjadi akan dapat dianalisa lebih lanjut dari sisi pandang analisa rasio dan keuangan perbankan

3. 3 Pengukuran dan Definisi Operasionalisasi Variabel

Untuk memberikan deskripsi yang lebih spesifik tehadap variabel penelitian ini maka variabel-variabel tersebut didefinisikan secara operasional sebagai berikut.

Hacking merupakan kegiatan mengakses atau menyusup ke sistem komputer dan

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

sistem elektronik tanpa hak. *Hacking* sebagai sebuah bentuk kegiatan kejahatan telah ada dan berkembang bersama perkembangan teknologi komputer dan internet. Variabel ini diukur berdasarkan pendapat para staf IT kantor perbankan dengan dimensi akses ilegal tanpa izin, pembajakan, melumpuhkan, dengan menggunakan skala ordinal 5 poin dari sangat tidak setuju (1), tidak setuju (2), netral (3), setuju (4) sampai sangat setuju (5).

Phising merupakan kegiatan memancing pemakai komputer di internet *(user)* agar mau memberikan informasi data diri pemakai *(username)* dan kata sandinya *(password)* pada suatu *website* yang sudah di-*deface*. *Phising* biasanya diarahkan kepada pengguna *online banking.* Isian data pemakai dan *password* yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya. Variabel ini diukur berdasarkan pendapat para staf IT kantor perbankan dengan dimensi variabel penipuan situs palsu, pencurian identitas dan memanipulasi tampilan layanan informasi dengan menggunakan skala ordinal 5 poin dari sangat tidak setuju (1), tidak setuju (2), netral (3), setuju (4) sampai sangat setuju (5).

Malware (malicious software) merupakan program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau *operating system. Malware* terdiri dari berbagai macam, yaitu: virus, *worm, trojan horse, adware, browser hijacker,* dll. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisipkannya di sebuah aplikasi ataupun file tertentu. Variabel ini diukur berdasarkan pendapat para staf IT kantor perbankan dengan menggunakan skala ordinal 5 poin dari sangat tidak setuju (1), tidak setuju (2), netral (3), setuju (4) sampai sangat setuju (5)..

IV. Hasil Dan Pembahasan

4.1. Uji Validitas

Uji Validitas dengan menggunakan bantuan dari software SPSS, dimana nilai validitas dapat dilihat pada kolom Corrected Item-Total Correlation. Jika nilai r hitung lebih besar dari r tabel dan nilai positif maka butir atau pertanyaan atau indikator tersebut valid (Ghozali, 2011). Dalam penelitian ini r tabel adalah n-2= 367 – 2 = 365 dengan taraf signifikan 5% maka r tabel untuk uji coba validitas dalam penelitian ini adalah 0,102. Berikut adalah hasil uji validitas variabel *hacking*, *phising* dan *malware*.

Berdasarkan Tabel 1 (lihat lampiran) dapat disimpulkan seluruh pertanyaan pada variabel *hacking* memiliki r hitung > 0,08, dan nilai signifikan < 0,05 maka dapat disimpulkan bahwa butir pertanyaan yang digunakan untuk mengukur variabel *hacking* dinyatakan valid.

Berdasarkan Tabel 2 (lihat lampiran) dapat disimpulkan seluruh pertanyaan pada variabel *phising* memiliki r hitung > 0,102, dan nilai signifikan < 0,05 maka dapat disimpulkan bahwa butir pertanyaan yang digunakan untuk mengukur variabel *phising* dinyatakan valid.

Berdasarkan Tabel 3 dapat disimpulkan seluruh pertanyaan pada variabel *malware* memiliki r hitung > 0,102, dan nilai signifikan dibawah 0,05 maka dapat disimpulkan bahwa butir pertanyaan yang digunakan untuk mengukur variabel *malware* dinyatakan valid.

Berdasarkan Tabel 4 dapat disimpulkan seluruh pertanyaan pada variabel *cyber security compliance* di Sektor Keuangan memiliki r hitung > 0,102, dan nilai signifikan dibawah 0,05 maka dapat disimpulkan bahwa butir pertanyaan yang digunakan untuk mengukur variabel *cyber security compliance* di Sektor Keuangan dinyatakan valid.

4.2. Uji Reliabilitas. Untuk mengukur suatu kuesioner yang merupakan indikator dari suatu variabel termasuk handal atau tidak. Untuk mengetahui reliabel atau tidaknya suatu variabel maka dilakukan uji statistik dengan cara melihat Cronbach's Alpha (α). Kriteria yang digunakan adalah suatu variabel dikatakan reliabel jika memberikan nilai α > 0,70 (Ghozali, 2011).

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Dari penyajian tabel diatas, maka seluruh variabel dinyatakan reliabel dimana hasil perhitungan uji reliabilitas menunjukan Cronbach's Alpha lebih besar dari 0,70.sehingga semua varibel dalam penelitian ini layak untuk dilanjutkan ke pengujian tahap selanjutnya.

4.3. Uji Normalitas.

Dilakukan menggunakan uji statistik non-parametik Kolmogorov-Smirnov (K-S) dengan melihat Asymp. Sig. (2-tailed) apakah lebih besar dari 0,05, jika lebih besar maka data terdistribusi normal (Ghozali,2011). Selain itu uji normalitas dapat dilihat dari grafik Normal P-P Plot. Berdasarkan hasil penelitian dapat dilihat nilai Asymp. Sig. (2-tailed) penelitian ini sebesar 0,201. Alpha pada kasus penelitian ini sebesar 5% sehingga dapat disimpulkan bahwa distribusi data dalam kasus penelitian ini terbukti normal. Dan juga dapat didukung dengan melihat grafik histogram dan grafik normal P-P PlRA dibawah ini. Berdasarkan gambar dibawah dapat disimpulkan bahwa model regresi ini memenuhi asumsi normalitas yaitu dimana dapat dilihat dari titik – titik yang mengikuti arah garis diagonal. Jika data menyebar di sekitar garis diagonal dan mengikuti arah garis diagonal, maka model regresi memenuhi asumsi normalitas (Ghozali, 2011).

4.4. Uji Multikolonieritas.

Bertujuan untuk menguji apakah model regresi ditemukan adanya korelasi antar variabel bebas (independen). Multikolonieritas dapat terlihat dari hasil Tolerance dan Variance Inflation Factor (VIF) yang terdapat dalam tabel Collinearity Statistic. Standar tidak terjadi multikolonieritas dalam penelitian ini adalah nilai Tolerance diatas 0,1 dan VIF kurang dari 10.

Berdasarkan hasil penelitian dapat dilihat bahwa nilai tolerance dari variabel *hacking* sebesar 0,884, phising sebesar 0,920 dan malware sebesar 0,948 lebih besar dari 0,1 dan nilai VIF dari variabel hacking sebesar 1,131, phising sebesar 1,086 dan malware sebesar 1,055 lebih kecil dari 10 sehingga dapat disimpulkan bahwa penelitian ini tidak terjadi multikolonieritas.

4.5. Uji Heteroskedastisitas.

Bertujuan menguji apakah dalam model regresi terjadi ketidaksamaan variance dari residual satu pengamatan ke pengamatan lainnya. Dalam penelitian ini untuk mendeteksi ada atau tidaknya heteroskedastisitas digunakan uji Glejser yang dapat dilihat dari nilai probabilitas signifikasinya atas tingkat kepercayaan 5% atau jika hasil uji signifikan Glejser ada yang dibawah 0,05 artinya terjadi heteroskedastisitas (Ghozali, 2011).

Dari hasil uji Glejser diatas menunjukan bahwa nilai sig untuk semua variabel > alpha dengan alpha 0,05. Dengan demikian tidak terjadi gejala heteroskedastisitas pada model ini dan didukung dengan grafik scatterplot diatas terlihat titik – titik menyebar secara acak, dengan demikian dapat disimpulkan bahwa tidak ada heteroskedastisitas pada model regresi ini.

4.6. Uji Statistik t.

Merupakan pengujian untuk menunjukkan seberapa jauh pengaruh satu variabel independen secara individual dalam menjelaskan variabel dependen. Hasil dapat dilihat dari tabel Coefficients dengan standar pengaruh signifikan jika nilai Signifikansi t lebih kecil dari alpha kasus penelitian.

Hipotesis Pertama penelitian menyatakan bahwa *hacking* berpengaruh positif terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan output spss yang terdapat pada tabel 8 terlihat bahwa variabel *hacking* memiliki t hitung sebesar 2,690 dan nilai signifikansi sebesar 0.007 < 0,05 sehingga H2 diterima. Hal ini menunjukkan bahwa *hacking* berpengaruh positif dan signifikan terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan hasil olah data menyatakan bahwa *hacking* berpengaruh secara positif dan signifikan terhadap *cybersecurity compliance* di sektor keuangan, dapat disimpulkan bahwa hipotesis pertama (H1) diterima.

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Hasil ini mendukung penelitian Derek Mohammed (2015) yang menyatakan bahwa *hacking* berpengaruh terhadap *cybersecurity compliance* di sektor keuangan. Secara harfiah hal ini sesuai dengan konsep sebab-akibat. Sesuatu tidak akan mungkin terjadi tanpa sebab yang jelas dan akibat apa yang akan ditimbulkan. Peningkatan kemanan siber *(cyber security)* khususnya pada sektor keuangan merupakan suatu tanggapan/respon pemerintah khususnya perbankan dalam menjaga keamanan sistem jaringan nasabahnya dari serangan-serangan siber. Jika perbankan selaku media penyimpanan aset para nasabah tidak dapat memberikan jaminan keamanan kepada nasabahnya maka hal ini akan merugikan para nasabah selaku orang yang menyimpan asetnya kepada bank.

Hipotesis kedua penelitian menyatakan bahwa *phising* berpengaruh positif terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan output spss yang terdapat pada tabel 8 terlihat bahwa variabel *phising* memiliki t hitung sebesar 5,983 nilai sig. sebesar 0.000 < 0.05 sehingga H2 diterima. Hal ini menunjukkan bahwa *phising* berpengaruh positif dan signifikan terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan hasil olah data menyatakan bahwa *phising* berpengaruh secara positif dan signifikan terhadap penerimaan opini audit *cybersecurity compliance* di sektor keuangan, dapat disimpulkan bahwa hipotesis kedua (H2) diterima. Hasil ini mendukung penelitian Intan Yuniar Purbasari (2012) yang menyatakan bahwa *phising* berpengaruh terhadap *cybersecurity compliance* di sektor keuangan. Tindak kejahatan ini merupakan kejahatan yang paling sering terjadi pada sektor keuangan nasabah bank khususnya. Dengan mencuri identitas nasabah maka sang pelaku dapat melakukan berbagai transaksi yang mengatasnamakan nasabah yang telah dicuri identitasnya. Hal ini membuat pemerintah selaku pihak yang berkuasa pada semua sektor dan aspek yang ada di Indonesia membuat kebijakan tentang kesadaran akan pentingnya *cyber security* tak terkecuali pada sektor keuangan.

Hipotesis ketiga penelitian menyatakan bahwa *malware* berpengaruh positif terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan output spss yang terdapat pada tabel 8 terlihat bahwa variabel *malware* memiliki t hitung sebesar 7,900 nilai sig. sebesar 0.000 < 0.05 sehingga H2 diterima. Hal ini menunjukkan bahwa *malware* berpengaruh positif dan signifikan terhadap *cybersecurity compliance* di sektor keuangan. Berdasarkan hasil olah data menyatakan bahwa *malware* berpengaruh secara positif dan signifikan terhadap penerimaan opini audit *cybersecurity compliance* di sektor keuangan, dapat disimpulkan bahwa hipotesis ketiga (H3) diterima. Hasil ini mendukung penelitian Tri Wahyu W. (2012) yang menyatakan bahwa *malware* berpengaruh terhadap *cybersecurity compliance* di sektor keuangan. Sesuai dengan penelitian yang dilakukan peneliti sebelumnya diatas, salah satu cara yang dapat dilakukan untuk mengamankan data dari anacaman malware adalah menginstall anivirus sebagai bentuk kepatuhan terhadap *cyber security.* Antivirus dapat digunakan untuk mengidentifikasi, mengkarantina, dan membuang *virus* dan *malware* lainnya yang terdapat pada sistem jaringan perbankan. Dengan memasang antivirus maka sistem jaringan dapat mengidentifikasi virus malware apa yang berpotensi menyerang dan merusak data nasabah perbankan sehingga langkah preventif selanjutnya dapat dilakukan.

4.7. Uji statistik F.

Merupakan model pengujian selain model pengujian stsistik t, pengujian ini untuk menunjukkan apakah semua variabel independen atau bebas dalam model penelitian mempunyai pengaruh terhadap variabel dependen. Hasil dapat dilihat dari tabel ANOVA dengan standar pengaruh signifikan jika nilai signifikansi F lebih kecil dari alpha kasus penelitian.

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Berdasarkan hasil uji F menunjukan bahwa F hitung sebesar 48,608 dengan nilai signifikansi sebesar 0,000. Nilai signifikansi tersebut lebih kecil dari pada tingkat signifikansi penelitian yaitu sebesar 0,05 maka dapat disimpulkan bahwa *hacking, phsing* dan *malware* berpengaruh secara signifikan terhadap variabel *cybersecurity compliance* di sektor keuangan.

4.8. Koefisien determinasi.

Koefisien determinasi yaitu mengukur seberapa jauh kemampuan model dalam menerangkan variasi variabel dependen. Nilai koefisien determinasi data dapat diperoleh dari hasil R-Square dengan kontrol nilai dari Adjusted R-Square. Untuk kontrol data yang baik, nilai Adjusted R-Square diharuskan positif.

Berdasarkan hasil penelitian ini, nilai Adjusted R-square sebesar 0,278 yang berarti variasi data yang ditimbulkan dari variabel *hacking, phising* dan *malware* terhadap variabel penerimaan opini audit going concern sebesar 27,8%. Sedangkan sisanya sebesar 72,2% berasal dari variabel-variabel lain diluar dari kasus ini. Kontrol data dalam penelitian ini juga dapat disimpulkan baik karena nilai adjusted R-square penelitian ini positif yaitu sebesar 0,278.

V. Simpulan Dan Saran

5.1. Simpulan.

Setelah dilakukan analisis atas penelitian pembahasan, maka diperoleh simpulan dari penelitian ini yaitu bahwa dalam dunia siber dibutuhkan kepatuhan terhadap aturan aturan yang berlaku dan diketahui untuk melindungi para pengguna siber itu sendiri, simpulan atas hipotesis yang diajukan dalam penelitian ini adalah : (1) *Hacking* berpengaruh positif dan signifikan terhadap *Cyber Security Compliance* di Sektor Keuangan. Hal ini menunjukkan bahwa semakin tinggi *Hacking*,atau semakin banyak pelaku dunia siber yang melakukan *hack* terhadap pengguna siber lainnya maka *Cyber Security Compliance* di Sektor Keuangan akan tinggi, dengan kata lain kepatuhan para pengguna siber untuk semakin memproteksi diri mereka dengan mematuhi aturan aturan dan ketentuan yang berlaku didunia siber akan semakin baik pula. (2) simpulan ini juga selaras dengan hiotesis kedua dan ketiga yang diajukan pada penelitian ini. *Phising* berpengaruh positif dan signifikan terhadap *Cyber Security Compliance* di Sektor Keuangan. Hal ini menunjukkan bahwa semakin tinggi *Phising*, maka *Cyber Security Compliance* di Sektor Keuangan akan tinggi. (3) *Malware* berpengaruh positif dan signifikan terhadap *Cyber Security Compliance* di Sektor Keuangan. Hal ini menunjukkan bahwa semakin tinggi *Malware*, maka *Cyber Security Compliance* di Sektor Keuangan akan tinggi. namun demikian penelitian ini memiliki keterbatasan terhadap jumlah responden yang dapat diakses pada sektor perbankan yang menjadi objek dalam penelitian ini, kehatian hatian pihak staf perbankan dalam menjaga dan merahasiakan informasi memiliki relasi terhadap keterbatasan dan keleluasaan responden dalam mengisi kuesioner ini.

5.2. Saran.

Berdasarkan kesimpulan dan keterbatasan penelitian diatas, maka penulis memberikan saran untuk penelitian selanjutnya, yaitu (1) Menambahkan variabel independen lainnya untuk mengetahui variabel – variabel lain yang mempengaruhi *cybersecurity compliance* di sektor keuangan. (2) Menambahkan jumlah sampel penelitian dan memperluas wilayah sampel penelitian sehingga hasil penelitian dapat memberikan gambaran yang lebih riil mengenai *cybersecurity compliance* di sektor keuangan. (3) Menjalin kerjasama secara formal kepada pihak perbankan dalam meningkatkan penelitian yang berhubungan dengan perbankan, sehingga akan mendapatkan hasil yang lebih reliabel dan terbebas dari *limited access*. Bagi peneliti selanjutnya, diharapkan dari hasil penelitian ini bisa dijadikan referensi dan sebagai bahan acuan penelitian yang sama dimasa yang akan datang mengenai *cybersecurity compliance* yang telah diteliti pada penelitian inin.

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Daftar Pustaka

Adenansi Retno dan Lia A.Novarina , (2017) Malware Dynamic, JOEICT (Jurnal of Education and Information Communication Technology) Volume 1, Nomor 1, Tahun 2017: 37 – 43

Adhi Dharma Aryyaguna. 2017. "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online". (Tidak Dipublikasikan). Universitas Hasanuddin.

Adi Pusdyanto (2008), Perilaku Hacker, (Tidak Dipublikasikan), Fakultas Psikologi Universitas Muhammadiyah Surakarta

Adlina Fikriyatun Nayyiroh dan Rizki Yudhi Dewantara. (2017). "Kesuksesan Implementasi Kebijakan Keamanan Sistem Informasi Sebagai Pencegah Cyber Crime". Jurnal Fakultas Ilmu Administrasi. Malang: Universitas Brawijaya.

Agus Raharjo. (2001). "Hacking Sebagai Fenomena Cybercrime". Tesis. Semarang: Universitas Diponegoro.

Agus Tri Prasetyo Harjoko. (2010). "Cyber Crime Dalam Perspektif Hukum Pidana". (tidak dipublikasikan). Surakarta: Universitas Muhammadiyah Surakarta.

Aidil dan Tri Wahyu W. Sanjaya . (2008). "Studi Sistem Keamanan Komputer". Jurnal Fakultas Teknologi Komunikasi dan Informatika. Pejaten: Universitas Nasional.

Anggriawan Egi dan Ryandi Yusuf. (2015). "Penerapan Metode Smart Authentication Dalam Layanan E-Banking Menggunakan Two Channel Authentication Dan QR-Code Pada Perangkat Mobile Android". Seminar Nasional. Bogor: Sekolah Tinggi Sandi Negara.

Augusty Ferdinand. (2014). "Metode Penelitian Manajemen", Edisi 5 2014. Diponegoro: Badan Penerbit Universitas Diponegoro.

Badrotuz Z., Diana K.P., Febri A.M., Putri R., Velenza R.P. (2014). "Economic of Crime". Jurnal Fakultas Ekonomi & Bisnis. Malang: Universitas Brawijaya.

Balian Zahab (2015) Modus modus kejahatan dalam tekhnologi informasi https://balianzahab.wordpress.com/

Cahya Febryan Permana.(2016). "Penerapan Metode Perception Untuk Pemilihan Serangan Oleh NPC Dalam Turn-Based RPG Game Pembelajaran Malware". (tidak dipublikasikan). Malang: Universitas Islam Negeri Maulana Malik Ibrahim.

Dian Rachmawati . (2014). "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber". Jurnal Fakultas Ilmu Komputer. Medan: Universitas Sumatera Utara.

Dodo Zaenal Abidin. (2015). "Kejahatan Dalam Teknologi Informasi dan Komunikasi". Jurnal Fakultas Ilmu Komputer. Jambi: STIKOM Dinamika Bangsa.

Dwi Chisva Islami dan Candiwan Khodijah Bunga I. H. (2016). "Kesadaran Keamanan Informasi Pada Bank X Di Bandung Indonesia". Jurnal Fakultas Komputer. Bandung: Universitas Telkom.

Eliasta Ketaren (2016), Cybercrime, Cyber Space, dan Cyber Law, Jurnal TIMES , Vol. V No 2 : 35-42 , 2016 ISSN : 2337 - 3601

Erick Lamdompak S. (2016). "Klasifikasi Malware Trojan Ransomware Dengan Algoritma Support Vector Machine (SVM)". Jurnal Fakultas Ilmu Komputer. Palembang: Universitas Sriwijaya.

Fana Akbarkan. (2007). "Tindak Pidana Hacking dan Cracking". (tidak dipublikasikan). Surabaya: Universitas Airlangga.

Handrini Ardiyanti (2014), "Cyber-Security Dan Tantangan Pengembangannya di Indonesia" Jurnal Politica Vol. 5 No. 1 Juni 2014

Haq, Kamar (2018) "What is Cyber Security?'Britania Educational Publishing New York ISBN 9781680488555 (ebook)

Haryo Andi Setiaji. (2016). "Tinjauan Hukum Internasional Terhadap Kasus Hacking Sony Pictures Entertainment". (tidak dipublikasikan). Universitas Hasanuddin.

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Hayati Mia Wibowo dan Nur Fatimah. (2017). "Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime". Jurnal Fakultas Ilmu Komputer. Tulungagung: STKPI PGRI Tulungagung.

Imam Ghozali. (2011). "Aplikasi Analisis Multivariete Dengan Program SPSS 21". Semarang: Badan Penerbit Universitas Diponegoro.

Intan Yuniar Purbasari. (2012). "Tinjauan Isu Keamanan Jaringan Komputer Di Tempat Kerja". Jurnal Fakultas Teknologi Industri. Surabaya: Universitas Pembangunan Nasional Veteran.

Khairul Anam (2010), Hacking vs Hukum Positif & Hukum Islam, Sunan Kalijaga Press, UIN Sunan Kalijaga Yogyakarta

McGuire, Mike, and Samantha Dowling, (2013) Cyber crime: A review of the evidence Chapter 4: Improving the cyber crime evidence base

Meeting the cyber security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory http://dakaadvisory.com/ wp-content/uploads/DAKA-Indonesiacyber-security-2013-web-version.pdf diakses 12 may 2018 2014 pukul 05.30 WIB

Michael Barama. (2011). "Elektronik Sebagai Alat Bukti Dalam Cyber Crime". Karya Ilmiah. Manado: Universitas Sam Ratulangi.

Mohammed, Derek. (2015). "Cybersecurity Compliance in the Financial Sector". Journal of Internet Banking and Commerce. Florida: Saint Leo University.

Nazarudin Tianotak. (2011). "Urgensi Cyber Law Di Indonesia Dalam Rangka Penanganan Cyber Crime Di Sektor Perbankan". Jurnal Fakultas Hukum. Ambon: Universitas Pattimura.

Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

Prasetyo Anugroho, Idris Winarno, Nur Rosyid.(2010). "Klasifikasi E-mail Spam Dengan Metode Naive Bayes Classifier Menggunakan Java Programming". Jurnal Fakultas Ilmu Komputer. Surabaya: Institut Teknologi Sepuluh November.

Ramardhian Agus Triyono Sumardi.(2014). "Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali". Jurnal. Boyolali:

Retno Adenansi dan Lia A. Novarina. (2017). "Malware Dynamic". Jurnal Fakultas Ilmu Komputer. Tulungagung: STKPI PGRI Tulungagung.

Reza Zulfikar Ruslam. (2013). "Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO 27001/ISMS Pada PT. XYZ". Karya Akhir. Jakarta: Universitas Indonesia.

Ronald Thompson & William Cats Barril, (2003) Information Technology and Management, New York: Mc Graw Hill, 2003, hal.29

Rudi Hermawan. (2013). "Kesiapan Aparatur Pemerintah Dalam Menghadapi Cyber Crime Di Indonesia". Jurnal Fakultas Ilmu Komputer. Jakarta: Universitas Indraprasta PGRI Jakarta.

Sukma Indrajati. (2014). "Tinjauan Hukum Internasional Terhadap Cyber Espionage Sebagai Salah Satu Bentuk Cybercrime". Skripsi. Makassar: Universitas Hasanuddin.

Tri Wahyu W. (2008). "Studi Sistem Keamanan Komputer". Jurnal Fakultas Teknologi Komunikasi dan Informatika. Jakarta: Universitas Nasional.

Wasista Sigit dkk. (2012). "Aplikasi Firewall Terhadap Malware Pada Media Dinamis". Jurnal Fakultas Ilmu Komputer. Surabaya: Institut Teknologi Sepuluh November.

Jurnal Akuntansi Bisnis
Vol.11 (No.2) : Hal. 99-110 Th. 2018
ISSN: 1979-360X
E-ISSN: 2598-6767

Tabel 1
Uji Validitas Variabel *Hacking*

INSTRUMEN VARIABEL	ITEM	R HITUNG	R TABEL	KET
HACKING	H1	0,599	0,102	Valid
	H2	0,592	0,102	Valid
	H3	0,585	0,102	Valid
	H4	0,756	0,102	Valid
	H5	0,701	0,102	Valid
	H6	0,697	0,102	Valid
	H7	0,567	0,102	Valid
	H8	0,651	0,102	Valid
	H9	0,576	0,102	Valid
	H10	0,582	0,102	Valid

Tabel 2.
Uji Validitas Variabel *Phising*

INSTRUMEN VARIABEL	ITEM	R HITUNG	R TABEL	KET
PHISING	P1	0,844	0,102	Valid
	P2	0,894	0,102	Valid
	P3	0,722	0,102	Valid
	P4	0,749	0,102	Valid
	P5	0,815	0,102	Valid
	P6	0,794	0,102	Valid

Tabel 3.
Uji Validitas Variabel *Malware*

INSTRUMEN VARIABEL	ITEM	R HITUNG	R TABEL	KET
MALWARE	M1	0,912	0,102	Valid
	M2	0,917	0,102	Valid
	M3	0,874	0,102	Valid

Tabel 4.
Uji Validitas Variabel *Cybersecurity Compliance* Di Sektor Keuangan

INSTRUMEN VARIABEL	ITEM	R HITUNG	R TABEL	KET
CYBERSECURITY COMPLIANCE DI SEKTOR KEUANGAN	CSC1	0,588	0,102	Valid
	CSC2	0,660	0,102	Valid
	CSC3	0,703	0,102	Valid
	CSC4	0,758	0,102	Valid
	CSC5	0,740	0,102	Valid
	CSC6	0,639	0,102	Valid
	CSC7	0,643	0,102	Valid
	CSC8	0,340	0,102	Valid
	CSC9	0,523	0,102	Valid

Tabel 5.
Uji Reliabilitas Variabel Penelitian

Variabel	Cronbach's Alpha	Batas Reliabilitas	Ket
Hacking	0,832	0,70	Reliabel
Phising	0,890	0,70	Reliabel
Malware	0,883	0,70	Reliabel
Cybersecurity Compliance di Sektor Keuangan	0,803	0,70	Reliabel