JURNAL BISNIS DAN AKUNTANSI
Vol. 10, No. 3, Desember 2008, Hlm. 113-126

INTENSITAS ANCAMAN KEAMANAN SISTEM INFORMASI AKUNTANSI KOMPUTERISASIAN

YULIUS KURNIA SUSANTO dan RATIH HANDAYANI

Trisakti School of Management, Jl. Kyai Tapa No.20 Grogol, Jakarta 11440,
siou_chiang@yahoo.com

The objective of the paper was (1) there are significant security threats of CAIS on the organization types, (2) there is difference among the organization types regarding the security threats of CAIS, (3) there are difference between integration-on line and integration-manual CAIS regarding the security threats of CAIS. Eighty four respondents from Jakarta organizations had participated in this research. The collecting data used a questionnaire survey via electronic-mail and post. Data were analyzed using a Kruskal-Wallis test. The results showed that first there is significant security threats of CAIS in Jakarta Organizations, like that the accidental entry of bad data, accidental destruction of data, employees' sharing of passwords and introduction of computer viruses the to CAIS are the significant security threats of CAIS in Jakarta Organizations. Second, there is no difference among the organization types regarding the security threats of CAIS. Third, there is no difference between integration-on line and integration-manual CAIS regarding the security threats of CAIS. But, there is difference between integration-on line and integration-manual CAIS regarding introduction of computer viruses to the CAIS.

Keywords: Security threats, information technology, computerized accounting information systems, integration.

PENDAHULUAN

Dewasa ini terjadi perubahan yang sangat drastis dalam teknologi informasi, yaitu berkembangnya sistem yang *user-friendly* dan keinginan perusahaan untuk memperoleh serta mengimplementasikan sistem komputer yang *up-to-date* dan *software* yang mudah digunakan. Perubahan tersebut diharapkan akan membuat tugas akuntansi menjadi lebih cepat dan akurat. Teknologi informasi mengalami perkembangan yang sangat cepat daripada tindaklanjut pengendalian dan perkembangan pengetahuan karyawan, keterampilan, kesadaran dan pemenuhan akan teknologi informasi.

Perubahan tersebut juga menyebabkan risiko keamanan yang berkaitan dengan sistem informasi akuntansi komputerisasian (SIAK) mengalami kenaikan (Erns & Young 1994). Seperti yang diungkapkan oleh Davis (1996), Erns & Young (1994) menyebutkan bahwa manager kadang-kadang mengorbankan keamanan sistem untuk menerapkan teknologi baru. Pengorbanan ini berdampak pada pelaporan keuangan eksternal dan pembuatan keputusan internal. Tanpa adanya tambahan keamanan, tidak akan menjamin kualitas informasi yang disediakan oleh sistem. Hal ini dapat mendatangkan masalah karena keputusan yang diambil berasal dari data yang tidak akurat dengan kemanan yang kurang.

Di sisi lain, kemajuan teknologi informasi juga menciptakan risiko yang signifikan terkait dengan keamanan dan integritas SIAK. Sering kita mendengar dan membaca berbagai publikasi yang terkait dengan ancaman keamanan SIAK seperti kesalahan data, informasi keuangan yang salah, pelanggaran terhadap pengendalian internal, pencurian, pembongkaran, kebakaran dan sabotase. Organisasi harus peduli dengan potensi ancaman keamanan yang mungkin dapat mengganggu SIAK mereka dan mengimplementasikan pengendalian keamanan untuk mencegah, mendeteksi dan mengkoreksi pelanggaran keamanan. Meskipun berbagai upaya sedapat mungkin telah dibuat oleh para praktisi akuntansi dalam mengurangi kerentanan SIAK bagi peristiwa semacam ini, usaha peningkatan keamanan SIAK harus tetap diperlukan (Abu-Musa 2003).

Sebelumnya penelitian ini telah dilakukan oleh berbagai peneliti antara lain Loch *et al*. (1992) yang menyebutkan bahwa ancaman keamanan SIAK yang paling besar berasal dari dalam perusahaan. Davis (1996) menyatakan bahwa sistem *microcomputer* dengan hubungan *network* keluar merupakan lingkungan yang paling tinggi tingkat risiko ancaman keamanan SIAK daripada lingkungan *mainframe* yang memiliki tingkat risiko yang rendah. Seperti yang diungkapkan oleh Abu-Musa (2004), Ryan dan Bordoloi (1997) menemukan adanya perbedaan ancaman keamanan SIAK antara lingkungan *client server* dan lingkungan *mainframe*. Sedangkan Henry (1997) melakukan survai pada perusahaan di Hampton Roads, Virginia, USA, untuk menentukan asal mula SIAK dan sistem kemanan yang mereka pakai.

Abu-Musa (2006) menemukan adanya ancaman keamanan SIAK atas organisasi sektor bank di Mesir dan juga menemukan bahwa tidak ada perbedaaan di antara organisasi sektor bank dalam kaitannya dengan berbagai ancaman keamanan yang mengganggu SIAK kecuali ancaman keamanan SIAK untuk akses data dan/ atau sistem secara tidak sah oleh pihak luar (*hacker*). Hasil penelitian tersebut konsisten dengan Abu-Musa (2004) yang melakukan penelitian di Arab Saudi, yang menyebutkan bahwa terdapat ancaman keamanan SIAK atas berbagai tipe organiasi yang berbeda dan juga tidak menemukan perbedaan ancaman keamanan SIAK di antara tipe organisasi yang berbeda.

Berdasarkan atas uraian hasil penelitian-penelitian sebelumnya, maka peneliti tertarik untuk menganalisis berbagai ancaman keamaman SIAK atas berbagai Organiasi yang ada di Jakarta, Indonesia, mengingat Indonesia merupakan negara berkembang yang SIAK-nya sama dengan negara berkembang lainnya seperti Arab Saudi dan Mesir.

Penelitian ini disusun dengan urutan penulisan sebagai berikut pertama, pendahuluan menjelaskan mengenai latar belakang masalah, tujuan penelitian dan organisasi penulisan. Kedua, deteksi *earnings management* dan hubungannya dengan relevansi nilai informasi akuntansi. Ketiga, metoda penelitian terdiri atas pemilihan sampel dan pengumpulan data, definisi operasional dan pengukuran variabel serta metoda analisis. Keempat, hasil penelitian yang berisi statistik deskriptif serta hasil dan interpretasi pengujian hipotesis. Terakhir, penutup yang berisi simpulan, keterbatasan penelitian dan saran untuk peneltian selanjutnya.

RERANGKA TEORITIS DAN PENGEMBANGAN HIPOTESIS

Ancaman keamanan sistem informasi akuntansi komputerisasian (SIAK) merupakan lingkup penelitian yang relatif baru karena masih kurangnya studi literatur mengenai penelitian ini khususnya di Indonesia. Aktivitas utama penelitian ini adalah: mendaftar ancaman keamanan yang mungkin mengganggu SIAK atas suatu organisasi; dan menemukan ancaman keamanan yang signifikan diterima. Salah satu penelitian yang paling penting dalam lingkup ini dikemukakan oleh Loch *et al*. (1992) yang menemukan bahwa persepsi sistem informasi manajemen (SIM) Eksekutif yang menyangkut ancaman keamanan dalam *microkomputer*, *mainframe computer* dan lingkungan *network*. Penelitian Loch *et al*. (1992) diarahkan pada dua pertanyaan yaitu apa sajakah yang mengancam sistem informasi dan data? dan manakah di antara ancaman tersebut merupakan ancaman paling serius?

Loch *et al*. (1992) mengembangkan daftar dua belas ancaman keamanan SIAK. Loch *et al*. (1992) menggunakan tiga metoda analisis data (*weighted votes, the number of first place votes and unit votes*) untuk mendeskripsikan keseluruhan makna dari ancaman keamanan SIAK. Hasil penelitian Loch *et al*. (1992) menunjukkan bahwa bencana alam dan ketidaksengajaan kesalahan karyawan terletak pada peringkat ancaman teratas yang diperoleh dari ketiga metoda. Hasil penelitian Loch *et al*. (1992) menyebutkan bahwa ancaman eksternal yang diterima lebih kecil daripada ancaman internal. Hasil ini memperkuat para ahli yang menyatakan bahwa ancaman terbesar berasal dari dalam perusahaan sendiri. Loch *et al*. (1992) juga menyatakan bahwa perusakan data secara tidak sengaja oleh karyawan, ketidaksengajaan memasukkan data yang salah oleh karyawan dan ketidakcukupan pengendalian melalui media penyimpanan sebagai ancaman yang paling penting dalam sebuah lingkungan *microcomputer*. Tiga ancaman yang paling penting pada *mainframe computer* adalah kesengajaan memasukkan data yang salah oleh karyawan, bencana alam, perusakan data secara sengaja oleh karyawan. Bencana alam, akses data/sistem oleh para *hacker* dan pengendalian yang lemah atau tidak efektif merupakan ancaman utama dalam lingkungan *network*.

Sejak keamanan SIAK menjadi salah satu perhatian utama dalam sistem informasi. Davis (1996) melakukan penelitian pada sejumlah sampel, yang secara random diambil dari anggota *Information Systems Audit and Control Association* (ISACA) dan *American Instituted of Certified Public Accountants* (AICPA). Hasil

penelitian Davis (1996) menunjukkan bahwa sebagian besar responden merasa bahwa ada sedikit tingkat risiko keamanan SIAK. Perbedaan lingkungan perkomputeran memiliki perbedaan tingkat risiko keamanan. Hal ini konsisten dengan penelitian Davis (1996) yang menunjukkan bahwa sistem *microcomputer* dengan hubungan *network* keluar merupakan lingkungan yang paling tinggi risiko ancaman keamanan SIAK, berbeda dengan lingkungan *mainframe* yang memiliki tingkat risiko paling rendah.

Belakangan ini, perkomputeran *client server* menjadi alternatif serius dalam perkomputeran *mainframe* pada beberapa organisasi. Meskipun sistem perkomputeran *client server* menawarkan beberapa keuntungan, mereka juga menunjukkan risiko tambahan dari lingkungan perkomputeran, yaitu fleksibilitas yang membuat mereka lebih menarik serta membuat mereka juga lebih rawan terhadap ancaman keamanan SIAK. Seperti yang diungkapkan oleh Abu-Musa (2004), Ryan dan Bordoloi (1997) menemukan bagaimana perusahaan berpindah dari *mainframe* menuju ke lingkungan *client server*. Tujuan penelitiannya adalah untuk memperoleh bukti empiris: (1) adanya perbedaan ancaman keamanan SIAK antara lingkungan *client server* dan *mainframe*; (2) Adanya perbedaan tingkat persiapan yang menyangkut perlindungan terhadap ancaman keamanan SIAK pada kedua lingkungan tersebut; (3) Adanya kesesuaian antara ukuran yang digunakan untuk mempersiapkan perlindungan terhadap ancaman keamanan SIAK dengan ancaman keamanan SIAK yang diterima pada kedua lingkungan tersebut.

Hasil penelitian Ryan dan Bordoloi (1997) menunjukkan bahwa dari lima belas ancaman keamanan SIAK, tujuh diantaranya berkaitan secara signifikan dengan lingkungan perusahaan. Kelemahan penelitian Ryan dan Bordoloi (1997), seperti yang diungkapkan oleh Abu-Musa (2004), adalah tidak jelas dalam membedakan antara ancaman kemanan SIAK dan ketidakcukupan pengendalian keamanan. Mereka memperlakukan beberapa ketidakcukupan pengendalian keamanan sebagai ancaman kemanan (seperti ketidakcukupan *trial audit* dan ketidakcukupan atau ketiadaan prosedur *logon*). Ryan dan Bordoloi (1997) juga menyatakan bahwa beberapa ancaman keamanan SIAK tidak dinyatakan dalam bentuk yang tegas. Meskipun demikian, mereka berargumen bahwa banyak ukuran kekuatan yang digunakan untuk menghadapi ancaman keamanan SIAK demi kelangsungan organisasi. Oleh karena itu, penelitian ini membedakan secara jelas antara ancaman kemanan dan pengendalian.

Henry (1997) melakukan survai pada perusahaan di Hampton Roads, Virginia, USA, untuk menentukan asal mula SIAK dan sistem kemanan yang mereka pakai. Ia berusaha mengetahui derajat koresponden antara teori dan praktik sesungguhnya dengan menggunakan tujuh cara perlindungan terhadap ancaman keamanan SIAK yaitu *encryption*, akses *password*, *backup* data, perlindungan terhadap virus, otorisasi bagi perubahan sistem, keamanan sistem fisik dan audit secara berkala.

Penelitian Abu-Musa (2006) menguji pendapat mengenai ancaman keamanan SIAK dari kepala bagian audit internal dan kepala bagian komputer pada organisasi Perbankan. Hasil penelitian Abu-Musa (2006) menunjukkan bahwa ketidaksengajaan memasukan data yang salah oleh karyawan, kesengajaan memasukan

data yang salah oleh karyawan, karyawan membagi-bagikan *password*, pengenalan virus komputer pada sistem, bencana alam dan ulah manusia, dan mencetak serta menyebarkan informasi secara langsung kepada seseorang yang tidak berhak untuk menerimanya, seluruhnya signifikan menjadi ancaman kemanan SIAK dalam organisasi Perbankan. Selain itu, Abu-Musa (2006) juga menyebutkan bahwa tidak ada perbedaaan di antara organisasi Perbankan dalam kaitannya dengan berbagai ancaman keamanan yang mengganggu SIAK kecuali ancaman keamanan SIAK untuk akses data dan/atau sistem secara tidak sah oleh pihak luar (*hacker*).

Hasil penelitian tersebut diperkuat oleh Abu-Musa (2004) yang melakukan penelitian di Arab Saudi, yang menyebutkan bahwa terdapat ancaman keamanan SIAK atas berbagai tipe organiasi yang berbeda. Abu-Musa (2004) juga tidak menemukan perbedaan ancaman keamanan SIAK di antara tipe organisasi yang berbeda.

Berdasarkan hasil penelitian-penelitian sebelumnya seperti yang telah diuraikan di atas, peneliti tertarik untuk melakukan penelitian tentang ancaman keamanan sistem informasi akuntansi komputerisasian atas berbagai tipe organisasi di Jakarta dengan menggunakan sembilan belas ancaman keamanan SIAK yang digunakan oleh Abu-Musa (2004). Dalam penelitian ini ditambahkan satu permasalahan yang tidak dibahas dalam penelitian Abu-Musa (2004) yaitu adakah perbedaan ancaman keamanan SIAK antara organisasi yang menggunakan SIAK yang terintegrasi dan SIAK yang terintegrasi-manual. Selain tipe organisasi dan kelompok responden, SIAK yang terintegrasi secara *on-line* akan lebih terbuka untuk mendapatkan ancaman keamanan SIAK daripada yang manual. Hipotesis-hipotesis yang diajukan adalah:

H_1: Terdapat ancaman keamanan yang paling mengganggu sistem informasi akuntansi komputerisasian atas berbagai tipe organisasi.

H_2: Terdapat perbedaan ancaman keamanan SIAK antar tipe organisasi yang berbeda.

H_3: Terdapat perbedaan ancaman keamanan SIAK antara organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual.

.

METODA PENELITIAN

Sampel diambil secara *purposive* dari berbagai tipe organisasi yang memiliki SIAK (Manufaktur, Perusahaan Jasa, Perbankan, Perdagangan Ritail, Pemerintah dan Pendidikan). *Purposive sampling* digunakan karena informasi yang akan diambil berasal dari sumber yang sengaja dipilih berdasarkan kriteria yang telah ditetapkan peneliti (Sekaran 2003). Kriteria yang ditetapkan adalah organisasi yang paling tidak sudah menggunakan sistem informasi akuntansi komputerisasian secara terintegrasi (*networking*) walaupun masih ada yang manual. Subjek penelitian ini adalah manager akuntansi. Mereka paling tidak sudah bekerja pada bidangnya selama dua tahun atau lebih.

Penelitian ini menggunaan internet untuk pengumpulan data dengan jalan menyebarkan kuisioner melalui *electronic-mail* dan pernah dipraktikkan dalam

penelitian Achyari (2000). Pengumpulan data juga menggunakan jasa pos. Jumlah kuisioner yang berhasil diperoleh sebanyak sembilan puluh empat kuisioner dan yang memenuhi kriteria penelitian sebanyak delapan puluh tiga kuisioner. Penggunaan *e-mail* dapat dijadikan sebagai tanda bahwa organisasi telah menggunakan sistem informasi akuntansi komputerisasian yang terintegrasi. Untuk memastikannya dalam kuisioner ditanyakan apakah organisasi sudah menggunakan sistem informasi akuntansi komputerisasian yang terintegrasi.

Secara umum ada empat jenis ancaman keamanan SIAK yang dihadapi oleh perusahaan yaitu: kehancuran karena bencana alam dan politik, kesalahan pada *software* dan tidak berfungsinya peralatan, tindakan yang tidak disengaja, dan tindakan yang disengaja (Romney dan Steinbart 2003). Penelitian ini menggunakan sembilan belas item ancaman keamanan sistem informasi akuntansi komputerisasian (SIAK) yang pernah digunakan oleh Abu-Musa (2004).

Pengukuran kesembilan belas ancaman keamanan SIAK tersebut menggunakan lima skala untuk mengukur intensitas ancaman keamanan SIAK yaitu setiap tahun atau tidak pernah, setiap bulan, setiap minggu, setiap hari dan lebih dari sekali dalam sehari atau lebih sering. Responden diminta untuk memberi skala intensitas setiap ancaman keamanan SIAK atas organisasi mereka.

HASIL PENELITIAN

Demografi responden dapat dilihat pada Tabel 1 sebagai berikut:

Tabel 1 Demografi Responden

Kriteria	Jumlah	Prosentase
Sektor Industri		
Manufaktur	23	27,7%
Perusahaan Jasa	19	22,9%
Perbankan	11	13,3%
Perdagangan Ritail	10	12%
Pemerintah	10	12%
Pendidikan	10	12%
Jumlah Akuntan		
1-5	56	67,5%
6-10	12	14,5 %
11-15	6	7,2%
16-20	9	10,8%
Jumlah Ahli Sistem Informasi		
1-5	65	78,3%
6-10	13	15,7 %
11-15	2	2,4%
16-20	3	3,6%

Aktivitas Penyebab Kerugian Keuangan		
Aktivitas dalam organisasi	31	37,3%
Aktivitas luar organisasi	22	26,5 %
Aktivitas dalam dan luar organisasi	20	24,1%
Aktivitas tidak keduanya	10	12%
Sistem Informasi Akuntansi Komputerisasian		
Organisasi yang menggunakan SIAK yang		
terintegrasi secara manual	60	72,3%
terintegrasi secara *on-line*.	23	27,7%

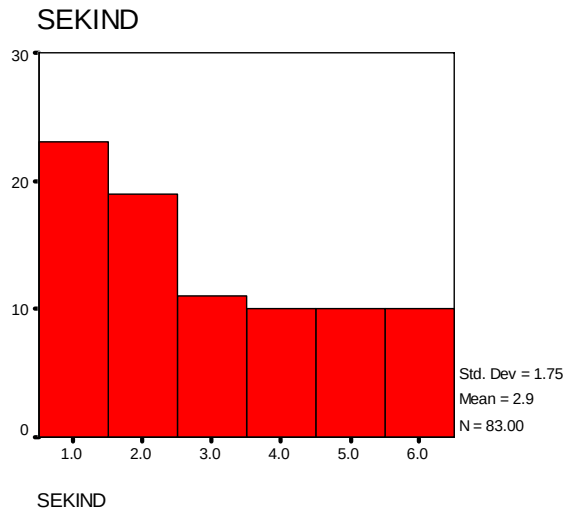
Sumber: Hasil Olah Data

Berdasarkan Tabel 1 dapat dilihat bahwa industri yang paling banyak adalah industri manufaktur sebesar 27,7% dengan jumlah akuntan dan ahli sistem informasi sebanyak 1 sampai 5 orang sebesar 67,5% dan 78,3%. Kerugian keuangan potensial akibat ancaman keamanan sistem informasi akuntansi komputerisasian (SIAK) adalah berasal dari aktivitas dalam perusahaan seperti tindakan karyawan sebesar 37,3% dan sistem informasi akuntansi yang paling banyak digunakan oleh perusahaan adalah terintegrasi secara manual sebesar 72,3%.

Sampel yang diperoleh berasal dari berbagai organisasi yang berbeda (lihat Gambar 1), aktivitas penyebab kerugian keuangan (lihat Gambar 2) dan organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual (lihat Gambar 3).

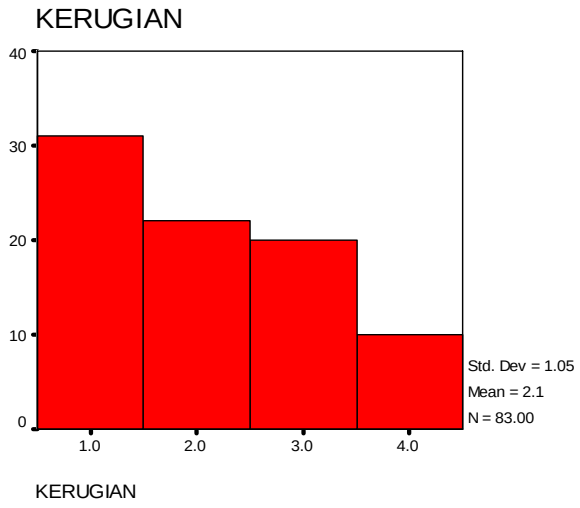
Pengujian hipotesis satu ditunjukkan dengan intensitas ancaman keamanan (lihat Tabel 2). Semakin sering ancaman keamanan terjadi maka ancaman tersebut mengganggu SIAK (Abu-Musa 2004, 2006). Dalam penelitian ini intensitas ancaman keamanan yang mengganggu SIAK adalah setiap hari. Dengan asumsi apabila ancaman keamanan tersebut terjadi setiap hari maka akan mengganggu SIAK. Berdasarkan Tabel 2, ancaman keamanan yang mengganggu SIAK adalah ketidaksengajaan memasukan data yang salah oleh karyawan, perusakan data secara tidak sengaja oleh karyawan, karyawan membagi-bagikan *password* dan pengenalan (masuknya) virus komputer pada sistem.

Ancaman keamanan yang mengganggu SIAK untuk industri Manufaktur adalah ketidaksengajaan memasukan data yang salah oleh karyawan; Untuk industri Jasa adalah ketidaksengajaan memasukan data yang salah oleh karyawan, perusakan data secara tidak sengaja oleh karyawan dan pengenalan (masuknya) virus komputer pada sistem; Untuk industri Perbankan adalah ketidaksengajaan memasukan data yang salah oleh karyawan, perusakan data secara tidak sengaja oleh karyawan, karyawan membagi-bagikan *password* dan pengenalan (masuknya) virus komputer pada sistem; Untuk industri Perdagangan Ritail adalah karyawan membagi-bagikan *password* dan pengenalan (masuknya) virus komputer pada sistem; Untuk Pemerintah adalah ketidaksengajaan memasukan data yang salah oleh karyawan, perusakan data secara tidak sengaja oleh karyawan dan pengenalan (masuknya) virus komputer pada sistem; Unutuk industri Pendidikan adalah pengenalan (masuknya) virus komputer pada sistem.



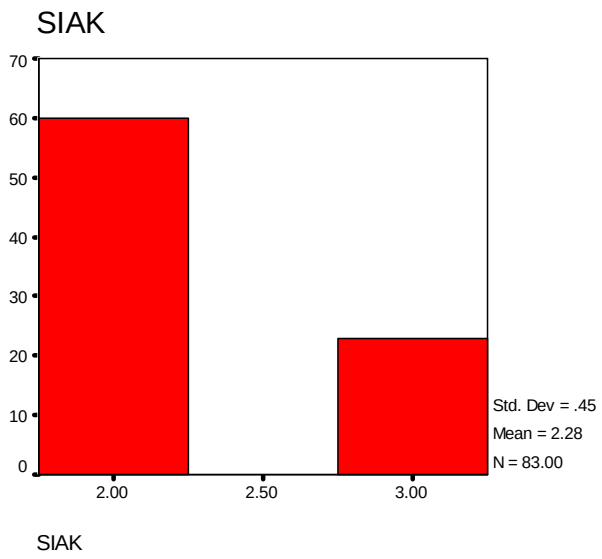
Keterangan: 1 Manufaktur, 2 Perusahaan Jasa, 3 Perbankan, 4 Perdagangan ritail, 5 Pemerintah dan 6 Pendidikan.

Gambar 1 Tipe Organisasi



Keterangan: 1 Kerugian keuangan berasal dari aktivitas dalam organisasi, 2 Kerugian keuangan berasal dari aktivitas luar organisasi, 3 Kerugian keuangan berasal dari aktivitas dalam dan luar organisasi, 4 Kerugian keuangan berasal dari aktivitas tidak keduanya.

Gambar 2 Aktivitas Penyebab Kerugian Keuangan



Keterangan: 2 Organisasi yang menggunakan SIAK yang terintegrasi secara manual dan 3 terintegrasi secara *on-line*.

Gambar 3 Sistem Informasi Akuntansi Komputerisasian

Tabel 2 Intensitas Ancaman Keamanan SIAK

	Ancaman Keamanan Sistem Informasi Akuntansi Komputerisasian	Setiap tahun atau tidak pernah		Setiap bulan		Setiap minggu		Setiap hari		lebih sering	
		n	%	n	%	n	%	n	%	n	%
1.	Ketidaksengajaan memasukan data yang salah oleh karyawan	23	27,7	34	41	19	22,9	4	4,8	3	3,6
2.	Kesengajaan memasukan data yang salah oleh karyawan	75	90,4	6	7,2	2	2,4	0	0	0	0
3.	Perusakan data secara tidak sengaja oleh karyawan	49	59	24	28,9	7	8,4	0	0	3	3,6
4.	Perusakan data secara sengaja oleh karyawan	81	97,6	2	2,4	0	0	0	0	0	0
5.	Akses data dan/atau sistem secara tidak sah oleh karyawan	70	84,3	11	13,3	2	2,4	0	0	0	0
6.	Akses data dan/atau sistem secara tidak sah oleh pihak luar (*hacker*)	79	95,2	4	4,8	0	0	0	0	0	0
7.	Karyawan membagi-bagikan *password*	67	80,7	10	12	2	2,4	4	4,8	0	0
8.	Bencana alam seperti kebakaran, banjir dan gempa bumi	60	72,3	22	26,5	1	1,2	0	0	0	0
9.	Bencana ulah manusia seperti kebakaran, teroris dan listrik padam	61	73,5	19	22,9	3	3,6	0	0	0	0
10.	Pengenalan (masuknya) virus komputer pada sistem	35	42,2	36	43,4	5	6	1	1,2	6	7,2
11.	Perusakan output	65	78,3	17	20,5	1	1,2	0	0	0	0
12.	Pembuatan output yang salah	59	71,1	22	26,5	2	2,4	0	0	0	0
13.	Pencurian data/informasi	79	95,2	4	4,8	0	0	0	0	0	0
14.	Penyalinan output secara tidak sah	78	94	4	4,8	1	1,2	0	0	0	0
15.	Penampilan dokumen pada monitor atau hasil cetakan yang bukan wewenangnya	70	84,3	13	15,7	0	0	0	0	0	0
16.	Pencetakan dan penyebaran informasi oleh seseorang yang tidak berwenang	77	92,8	6	7,2	0	0	0	0	0	0
17.	Mencetak dan menyebarkan informasi secara langsung kepada orang yang tidak berhak untuk menerimanya	72	86,7	10	12	1	1,2	0	0	0	0
18.	Pemusnahan (*shredding*) dokumen yang diserahkan kepada seseorang yang tidak jelas keamanannya	77	92,8	4	4,8	2	2,4	0	0	0	0
19.	Penahanan transmisi data dari lokasi yang berbeda	75	90,4	6	7,2	2	2,4	0	0	0	0

Sumber: Hasil Olah Data

Hasil ini mendukung penelitan Abu-Musa (2004 dan 2006) yang menyebutkan bahwa ketidaksengajaan dan kesengajaan memasukan data yang salah oleh karyawan, ketidaksengajaan perusakan data oleh karyawan, karyawan membagi-bagikan *password*, becana alam maupun ulah manusia, pengenalan virus komputer pada sistem, perusakan output, penampilan dokumen pada monitor atau hasil cetakan yang bukan wewenangnya, pencetakan langsung dan distribusi informasi kepada orang yang tidak berhak untuk menerimanya adalah ancaman keamanan yang mengganggu SIAK di organisasi Arab Saudi.

Berdasarkan Tabel 3, hasil pengujian hipotesis dua menunjukkan bahwa tidak ada perbedaan ancaman keamanan SIAK antar tipe organisasi yang berbeda sehingga hipotesis dua tidak terdukung. Hasil pengujian hipotesis dua mengindikasikan bahwa hampir semua tipe organisasi di Jakarta mengalami ancaman keamanan SIAK yang sama. Hasil temuan ini mendukung penelitian Abu-Musa (2004, 2006) yang menyebutkan tidak ada perbedaan antar tipe organisasi yang berbeda dalam kaitannya dengan intensitas ancaman keamanan SIAK pada organisasi di Arab Saudi dan Mesir.

Tabel 3
Hasil *Kruskal-Wallis Test* untuk Tipe Organisasi

	Ancaman Keamanan Sistem Informasi Akuntansi Komputerisasian	*Chi-Square*	*df*	*Asymp. Sig.*
1.	Ketidaksengajaan memasukan data yang salah oleh karyawan	2,807	5	0,730
2.	Kesengajaan memasukan data yang salah oleh karyawan	3,147	5	0,677
3.	Perusakan data secara tidak sengaja oleh karyawan	5,317	5	0,378
4.	Perusakan data secara sengaja oleh karyawan	4,003	5	0,549
5.	Akses data dan/atau sistem secara tidak sah oleh karyawan	1,100	5	0,954
6.	Akses data dan/atau sistem secara tidak sah oleh pihak luar (*hacker*)	2,030	5	0,845
7.	Karyawan membagi-bagikan *password*	5,352	5	0,374
8.	Bencana alam seperti kebakaran, banjir dan gempa bumi	3,550	5	0,616
9.	Bencana ulah manusia seperti kebakaran, teroris dan listrik padam	6,574	5	0,254
10.	Pengenalan (masuknya) virus komputer pada sistem	1,502	5	0,913
11.	Perusakan output	3,828	5	0,574
12.	Pembuatan output yang salah	8,425	5	0,134
13.	Pencurian data/informasi	7,751	5	0,171
14.	Penyalinan output secara tidak sah	1,704	5	0,888
15.	Penampilan dokumen pada monitor atau hasil cetakan yang bukan wewenangnya	2,463	5	0,782
16.	Pencetakan dan penyebaran informasi oleh seseorang yang tidak berwenang	5,015	5	0,414
17.	Mencetak dan menyebarkan informasi secara langsung kepada orang yang tidak berhak untuk menerimanya	0,986	5	0,964
18.	Pemusnahan (*shredding*) dokumen yang diserahkan kepada seseorang yang tidak jelas keamanannya	3,172	5	0,673
19.	Penahanan transmisi data dari lokasi yang berbeda	2,119	5	0,832

Sumber: Hasil Olah Data

Tabel 4 memberikan bukti empiris bahwa secara keseluruhan tidak ada perbedaan antara organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual. Akan tetapi pengenalan (masuknya) virus komputer pada sistem (*Asymp.Sig.*=0,013) merupakan ancaman keamanan SIAK yang berbeda antara organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual. Ancaman pengenalan (masuknya) virus komputer pada sistem sering terjadi pada organisasi yang SIAK terintegrasi secara *on-line* daripada terintegrasi secara manual (lihat Tabel 5 pada AK10). Hal ini menunjukkan bahwa SIAK yang terintegrasi secara *on-line* sangat rentan untuk masuknya virus komputer pada sistem.

Tabel 4
Hasil *Kruskal-Wallis Test* untuk SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual

	Ancaman Keamanan Sistem Informasi Akuntansi Komputerisasian	*Chi-Square*	*df*	*Asymp. Sig.*
1.	Ketidaksengajaan memasukan data yang salah oleh karyawan	1,051	1	0,305
2.	Kesengajaan memasukan data yang salah oleh karyawan	1,049	1	0,306
3.	Perusakan data secara tidak sengaja oleh karyawan	0,000	1	0,991
4.	Perusakan data secara sengaja oleh karyawan	0,776	1	0,378
5.	Akses data dan/atau sistem secara tidak sah oleh karyawan	0,120	1	0,729
6.	Akses data dan/atau sistem secara tidak sah oleh pihak luar (*hacker*)	1,030	1	0,310
7.	Karyawan membagi-bagikan *password*	1,14	1	0,314
8.	Bencana alam seperti kebakaran, banjir dan gempa bumi	0,059	1	0,809
9.	Bencana ulah manusia seperti kebakaran, teroris dan listrik padam	3,098	1	0,078
10.	Pengenalan (masuknya) virus komputer pada sistem	6,162	1	0,013*
11.	Perusakan output	0,308	1	0,579
12.	Pembuatan output yang salah	0,181	1	0,670
13.	Pencurian data/informasi	0,015	1	0,902
14.	Penyalinan output secara tidak sah	0,366	1	0,545
15.	Penampilan dokumen pada monitor atau hasil cetakan yang bukan wewenangnya	0,879	1	0,349
16.	Pencetakan dan penyebaran informasi oleh seseorang yang tidak berwenang	1,585	1	0,208
17.	Mencetak dan menyebarkan informasi secara langsung kepada orang yang tidak berhak untuk menerimanya	0,004	1	0,952
18.	Pemusnahan (*shredding*) dokumen yang diserahkan kepada seseorang yang tidak jelas keamanannya	1,416	1	0,234
19.	Penahanan transmisi data dari lokasi yang berbeda	0,344	1	0,557

*=sig.<0,05

Sumber: Hasil Olah Data

Tabel 5
***Mean Rank* untuk SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual**

	AK1	AK2	AK3	AK4	AK5	AK6	AK7	AK8	AK9	AK10
On-line (n=23)	46,15	39,76	41,96	41,00	41,07	43,61	44,96	41,20	36,2	51,74
Manual (n=60)	40,41	42,86	42,02	42,38	42,36	41,38	40,87	42,31	44,22	38,27

Sumber: Hasil Olah SPSS

	AK11	AK12	AK13	AK14	AK15	AK16	AK17	AK18	AK19
On-line (n=23)	43,0	40,57	41,80	43,07	44,52	44,41	41,85	44,8	43,28
Manual (n=60)	41,35	42,55	42,08	41,59	41,03	41,08	42,06	41,13	41,51

Sumber: Hasil Olah Data

PENUTUP

Tujuan utama dari penelitian ini adalah untuk menyelidiki ancaman keamanan yang signifikan diterima oleh sistem informasi akuntansi komputerisasian (SIAK), melalui intensitas keterjadian mereka dalam berbagai organisasi di Jakarta. Daftar ancaman keamanan SIAK yang digunakan telah dikembangkan berdasarkan penelitian sebelumnya (sebagai contoh, Loch *et al.*1992, Davis 1996, Henry 1997, Abu-Musa 2004, 2006).

Hasil penelitian memberikan tiga bukti empiris, yaitu pertama, terdapat ancaman keamanan yang mengganggu SIAK adalah ketidaksengajaan memasukan data yang salah oleh karyawan, perusakan data secara tidak sengaja oleh karyawan, karyawan membagi-bagikan *password* dan pengenalan (masuknya) virus komputer pada sistem. Kedua, tidak ada perbedaan ancaman keamanan SIAK antar tipe organisasi yang berbeda.

Terakhir, secara keseluruhan tidak ada perbedaan antara organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual. Akan tetapi pengenalan (masuknya) virus komputer pada sistem merupakan ancaman keamanan SIAK yang berbeda antara organisasi yang menggunakan SIAK yang terintegrasi secara *on-line* dan terintegrasi secara manual. Ancaman pengenalan (masuknya) virus komputer pada sistem sering terjadi pada organisasi yang SIAK terintegrasi secara *on-line* daripada terintegrasi secara manual.

Implikasi penelitian ini adalah bahwa pengelola organisasi akan lebih memperhatikan ancaman-ancaman keamanan yang terkait dengan sistem informasi akuntansi komputerisasian (SIAK) terlebih pada ancaman pengenalan (masuknya) virus komputer pada sistem. Pengelola Oganisasi perlu meng-*update software* antivirus terlebih pada virus yang merusak jejaring SIAK. Bagi karyawan yang pekerjaannya terkait dengan SIAK akan lebih berusaha untuk mengatasi berbagai ancaman keamanan yang mengganggu jalannya kegiatan SIAK, seperti tidak cerobah dalam mengelola data dan/atau sistem.

Keterbatasan penelitian ini adalah jumlah sampel untuk tiap tipe organisasi yang kurang proposional serta sedikitnya sampel yang diperoleh. Hal ini disebabkan oleh kuisioner yang dikirimkan banyak tidak direspon, mengingat responden yang digunakan, yaitu manajer akuntansi. Untuk penelitian selanjutnya sebaiknya menggunakan responden karyawan akuntansi dan keuangan yang terlibat langsung dengan SIAK. Keterbatasan lainnya adalah daftar ancaman keamanan SIAK yang digunakan adalah sembilan belas butir. Menurut responden masih ada ancaman keamanan SIAK lainnya yang terjadi di perusahaan mereka tetapi tidak teridentifikasi dalam penelitian ini, seperti ketidakjujuran karyawan, kesalahan data inputan dari nasabah, kesalahpahaman penyampaian informasi dan kelupaan *backup* data. Untuk penelitian selanjutnya mempertimbangkan ancaman keamanan tersebut.

Hasil penelitian ini tidak dapat digeneralisasi untuk semua industri di Jakarta. Bagaimanapun, penelitian lebih lanjut perlu dilakukan dengan menambah jumlah sampel untuk memperluas dan mengembangkan penelitian ini. Penelitian yang lebih jauh dibutuhkan untuk menunjukkan bukti empiris dari daerah lainnya seperti Medan, Semarang dan Surabaya yang *notabene*-nya daerah tersebut merupakan salah satu pusat bisnis di Indonesia. Studi komparatif dapat diambil untuk menyelidiki perbedaan yang signifikan antara daerah satu dan daerah lainnya dalam kaitannya dengan penelitian isu keamanan SIAK.

REFERENSI:

Achyari, Didi. 2000. Pemanfaatan Internet untuk Riset dan Implikasi terhadap Riset Akuntansi. *Jurnal Ekonomi dan Bisnis Indonesia* 15 (2), hlm. 257-267.

Abu-Musa, Ahmad A. 2003. The Perceived Threats to the Security of Computerized Accounting Information Systems. *The Journal of American Academy of Business* Vol.3, No.1, September, hlm. 9-20.

Abu-Musa, Ahmad A. 2004. Exploring the Perceived Threats of Computerized Accounting Information Systems in Emerging Countries: an Emprical Study on Saudi Organizations. *European Accounting Information Systems Conference 2004*. Prague: Annual Congress of the European Accounting Association.

Abu-Musa, Ahmad A. 2006. Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry. *Journal of Information Systems* Vol.20, No.1 Spring, hlm. 187-203.

Davis, Charles E. 1996. Perceived Security Threats to today's Accounting Information Systems: a Survey of CISAs. *IS Audit & Control Journal* Vol.3, hlm. 38-41.

Febrian, Jack dan Farida Andayani 2002. *Kamus Komputer dan Istilah Teknologi Informasi*. Bandung: Penerbit Informatika Bandung.

Hair, J.F., Anderson, R.E., dan Black, W.C. 2006. *Multivariate Data Analysis*. Sixth Edition. New Jersy: Prentice Hall International, Inc.

Henry, Laurie 1997. A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia. *The Mind-Atlantic of Business.* Vol.33, Iss.69, hlm. 171-189.

Loch, Karen D., Houstan H. Carr dan Merrill E. Warkentin 1992. Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, Juni, hlm. 173-186.

Romney, B. Marshall dan Paul J. Steinbart. 2003. *Accounting Information Systems*. New Jersey: Pearson Education, Inc.

Sekaran, Uma. 2003. *Research Methods for Business: A Skill-Building Approach*. Fourth Edition. New York: John Wiley & Sons, Inc.