

FAKTOR-FAKTOR ANCAMAN KEAMANAN SISTEM INFORMASI AKUNTANSI

Nida Nusaibatul Adawiyah,
Fakultas Ekonomi Jurusan Akuntansi – Universitas Gunadarma
nida_n_adawiyah@staff.gunadarma.ac.id

ABSTRAK

Kemajuan tekonologi saat ini sangat membantu perusahaan atau organisasi dalam menjalankan aktivitasnya khususnya pada penggunaan sistem informasi akuntansi yang terkomputerisasi. Tujuan dari penelitian ini yaitu untuk mengetahui dan menganalisis ancaman keamanan yang paling mengganggu sistem informasi akuntansi dan mengetahui perbedaan ancaman keamanan sistem informasi akuntansi di beberapa sektor industri. di wilayah Jakarta, Bogor dan Tangerang. Metode analisis yang digunakan adalah analisis inferensial yaitu mendeskripsikan dan menggambarkan data yang telah terkumpul sebagaimana adanya yang kemudian akan di tarik kesimpulan yang berlaku untuk populasi. Hasil dari penelitian menyatakan bahwa ancaman kemanan sistem informasi yang paling mengganggu sistem informasi akuntansi yaitu seringnya karyawan berbagi password.

Kata kunci: Ancaman kemanan, sistem informasi akuntansi

PENDAHULUAN

Sistem informasi akuntansi merupakan elemen-elemen yang saling terhubung dengan rangkaian aktivitas yang dilakukan oleh perusahaan atau organisasi dalam mengumpulkan informasi-informasi secara terstruktur dalam menjalankan kegiatan operasional suatu organisasi yang nantinya akan dibutuhkan oleh pihak-pihak tertentu dan pihak manajemen untuk pengambilan keputusan, serta kebijakan. Pada negara berkembang, sistem informasi akuntansi komputerisasi sudah banyak digunakan. Melihat cepatnya pertumbuhan teknologi, maka menjaga keamanan terhadap sistem informasi juga sangat penting di perlukan. Survey menunjukan bahwa 67% perusahaan memiliki cabang keamanan, lebih dari 45% ditargetkan berdasarkan kejahatan yang terorganisasi, dan 80% dilaporkan merugi secara financial, (Steinbart, 2014: 145).

Tijani Oladipupo Muhtala, Mathias Ogundeji (2013) menunjukan

hasil penelitiannya mengenai ancaman sistem informasi akuntansi dalam perkembangan ekonomi di Nigeria bahwa mayoritas responden setuju dengan pernyataan bahwa *computerized accounting information system* ini terkena ancaman keamanan baik di dalam maupun di luar organisasi. Studi ini menemukan bahwa faktor-faktor seperti entri data yang buruk tanpa disengaja oleh karyawan, kerusakan data disengaja oleh karyawan, karyawan berbagi log-on kredensial, pengenalan virus, akses tidak sah kesistem informasi dan dokumen yang tidak sah, visibilitas melalui tampilan dimonitor dan dokumen hardcopy adalah ancaman keamanan yang paling signifikan untuk sistem informasi akuntansi terkomputerisasi.

Sistem informasi adalah cara-cara yang diorganisasikan untuk mengumpulkan, memasukan, mengolah dan menyimpan data, dan cara-cara yang diorganisasikan untuk menyimpan, mengelola, mengendalikan, dan melaporkan

informasi untuk mencapai tujuan (Krismiaji, 2010).

Sistem informasi akuntansi adalah sistem yang mengumpulkan, catatan, dan data proses untuk menghasilkan informasi bagi pengambil keputusan, (Romney dan Steinbart, 2012). Beberapa manfaat dan tujuan penting sistem informasi akuntansi pada sebuah organisasi antara lain :

1. Mengumpulkan dan menyimpan data tentang aktivitas dan transaksi
2. Memproses data menjadi informasi yang dapat digunakan dalam proses pengambilan keputusan
3. Melakukan pengendalian secara tepat terhadap asset organisasi.

Penggunaan sistem informasi akuntansi

Pada pembahasan ini, ada lima macam penggunaan sistem informasi, yaitu, (Dasaratha V.Rama/Frederick L.Jones, 2008) :

1. Membuat laporan eksternal
2. Mendukung aktivitas rutin
3. Mendukung pengambilan keputusan
4. Perencanaan dan pengendalian.
5. Menerapkan pengendalian internal

Pengendalian pusat komputer

Tujuan pengendalian pusat komputer adalah untuk mengkaji berbagai pengendalian yang didesain untuk mencegah dan mendeteksi bencana atas pusat komputer. Berikut ini adalah beberapa fitur pengendalian yang secara langsung dapat berkontribusi pada keamanan lingkungan pusat komputer, (Hall singleton, 2007).

1. Lokasi fisik

Lokasi fisik komputer secara langsung memengaruhi berbagai risiko bencana dan ketersediaan. Sebisa mungkin, sistem komputer jauh dari berbagai bahaya yang di timbulkan manusia dan alam, seperti pabrik pemrosesan, pipa gas dan air, bandara, wilayah yang tingkat

kejahatannya tinggi, dataran yang banjir, dan struktur geologi yang tidak tepat.

2. Kontruksi

Sebuah pusat komputer idealnya ditempatkan dalam sebuah bangunan berlantai satu yang konstruksinya solid dengan akses terkendali. Jika pusat komputer terpaksa berlokasi digedung yang terdiri dari beberapa lantai, maka seharusnya ditempatkan di lantai atas.

3. Akses

Akses ke pusat komputer seharusnya dibatasi hanya untuk operator dan karyawan lainnya yang bekerja ditempat tersebut. Pengendalian fisik seperti pintu yang terkunci, seharusnya digunakan untuk membatasi akses ke pusat tersebut atau dengan menggunakan keypad atau kartu gesek. Pusat komputer seharusnya juga menggunakan daftar masuk (*sign-in log*) bagi para programmer dan analis yang membutuhkan akses untuk memperbaiki kesalahan program. Pusat komputer harus memelihara catatan yang akurat atau lalu lintas yang semacam itu dengan orang-orang yang tidak bekerja tetap dipusat komputer , untuk memverifikasi pengendalian akses.

4. Pengatur suhu udara

Kesalahan dapat terjadi dalam piranti keras komputer jika suhu menyimpang jauh dari kisaran optimalnya. Selain itu risiko kerusakan sirkuit akibat gelombang listrik statis akan meningkat ketika kelembaban turun, sebaliknya kelembaban yang tinggi dapat menyebabkan jamur tumbuh.

5. Pemadam kebakaran

Ancaman bencana alam paling umum adalah kebakaran. Separuh dari perusahaan yang mengalami kebakaran bangkrut karena hilangnya berbagai catatan yang sangat penting.

6. Pasokan listrik

Pasokan listrik yang tiba-tiba menurun secara umum dapat dikendalikan dengan adanya cadangan baterai (*uninterruptible supply*). Keputusan berkaitan dengan pengendalian listrik dapat menjadi keputusan yang mahal dan biasanya membutuhkan saran serta analisis dari para ahli.

dimaksudkan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat kerusakan sistem. Secara garis besar, ancaman sistem informasi dapat dibagi menjadi dua macam, yaitu ancaman aktif dan ancaman pasif. Ancaman aktif melingkupi kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia, dan bencana alam. Kegagalan sistem menyatakan kegagalan terhadap sistem informasi, (Abdul Kadir, 2014). Empat jenis ancaman SIA yang dihadapi perusahaan diringkas dalam tabel 1

Ancaman keamanan sistem informasi akuntansi

Keamanan merupakan faktor penting yang harus diperhatikan dalam pegerasian sistem informasi, yang

Tabel 1 Ancaman untuk sistem informasi akuntansi

Ancaman	Contoh
Bencana alam dan politik	Kebakaran atau panas berlebihan Banjir, gempa bumi, longsor, topan, tornado, badai salju, dan hujan yang membekukan Perang dan serangan teroris
Kesalahan perangkat lunak dan kegagalan fungsi peralatan	Kegagalan perangkat keras dan perangkat lunak Kesalahan perangkat lunak atau <i>bugs</i> Benturan sistem operasi Pemadaman listrik dan fluktuasi
Tindakan yang tidak diharapkan	Kesalahan transmisi data yang tidak terdeteksi Kecelakaan yang disebabkan oleh kelalaian manusia, kegagalan untuk mengikuti prosedur yang ditetapkan, dan personel yang dilatih atau diawasi dengan buruk Kesalahan atau kelalaian yang tidak diinginkan Kehilangan, kesalahan, kerusakan atau salah menempatkan data Kesalahan logika Sistem yang tidak memenuhi kebutuhan perusahaan atau tidak bisa menangani tugas yang diajukan Sabotase
Tindakan yang disengaja (kejahatan komputer)	Misrepresentasi, penggunaan yang salah atau pengungkapan data yang tidak diotorisasi Penyalahgunaan asset Penipuan laporan keuangan Penipuan laporan keuangan Korupsi Penipuan komputer - serangan rekayasa sosial, malware, dll

Steinbart (2014).

METODE PENELITIAN

Objek Penelitian

Objek yang digunakan dalam penelitian ini adalah beberapa jenis perusahaan, antara lain manufaktur, bank, asuransi, kesehatan, perdagangan, pemerintahan, dan lain-lain.

Populasi dan Sampel

Populasi penelitian pada penelitian yaitu di wilayah Jakarta, Bogor, Tangerang. Sampel yang digunakan terdiri dari pengguna sistem informasi akuntansi di setiap perusahaan objek penelitian. Teknik sampling yang digunakan adalah simpel random sampling.

Data yang digunakan

Data yang digunakan dalam penelitian ini yaitu data mengenai persepsi seluruh pengguna di masing-masing perusahaan terhadap ancaman yang mengganggu sistem informasi akuntansi dalam bentuk pengisian kuesioner dan gambaran tentang perusahaan meliputi jenis perusahaan, jumlah akuntan profesional, jumlah spesialis sistem informasi, jabatan, lama bekerja, sistem akuntansi yang digunakan, dan kerugian secara materi yang diakibatkan dari gangguan sistem. Parameter pengukuran frekuensi ancaman keamanan sistem informasi akuntansi di beberapa perusahaan mengacu pada jurnal sebelumnya menggunakan 19 parameter, dapat dilihat pada tabel 2

Tabel 2 Parameter Ancaman Sistem Informasi Akuntansi

No	Ancaman
1	Bencana alam seperti banjir, kebakaran, dll
2	Entri data yang buruk di sengaja oleh karyawan
3	Kerusakan data tanpa disengaja oleh karyawan
4	Kerusakan data yang disengaja oleh karyawan
5	Akses tidak sah ke data dan/ atau sistem oleh karyawan
6	Akses tidak sah ke data dan/ atau sistem oleh orang luar/ hacker
7	Karyawan berbagi password
8	Bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya SIA
9	Perusakan atau hancurnya output sistem (interupsi)
10	Penciptaan output fiktif/ output salah
11	Pencurian data dan/ atau informasi
12	Menyalin file output tanpa izin
13	Visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak
14	Mencetak file dan di distribusi oleh orang yang tidak berwenang
15	Cetakan dan informasi di arahkan oleh orang yang tidak berwenang
16	Entri data yang buruk tanpa sengaja oleh karyawan Fabrikasi (memasukan pesan palsu, memasukan data palsu, menyerahkan dokumen kepada orang yang tidak di otorisasi)
17	
18	Masuknya virus komputer ke sistem
19	Intersepsi transmisi data dari lokasi jarak jauh

Parameter ancaman keamanan sistem informasi akuntansi pada tabel 2 merupakan rujukan jurnal penelitian yang ditulis oleh Abu Musa dengan judul “*Investigating the Perceived Threats of Computirezed Accounting Information System in Developing Countries : An Empirical Study on Saudi Arabia Organization*” pada tahun 2006. Pengukuran frekuensi terjadi ancaman tersebut dilihat dari intensitasnya yaitu kurang dari satu tahun, Satu tahun untuk bulanan, Satu bulan untuk mingguan, Seminggu untuk sehari-hari, dan Harian atau lebih sering.

Analisis Data

Pada penelitian ini, analisis data yang digunakan untuk menganalisis dan mengkaji ancaman keamanan yang

paling mengganggu pada sistem informasi akuntansi adalah analisis inferensial yaitu mendeskripsikan dan menggambarkan data yang telah terkumpul sebagaimana adanya yang kemudian akan di tarik kesimpulan yang berlaku untuk populasi. Untuk menganalisis ancaman yang paling mengganggu keamanan sistem informasi akuntansi adalah dengan meranking ancaman yang memiliki nilai paling besar menurut persepsi pengguna sistem informasi akuntansi.

HASIL DAN PEMBAHASAN

Jenis perusahaan

Pada data jenis perusahaan, peneliti mengambil objek pada sembilan perusahaan yang dapat dilihat pada tabel 3.

Tabel 3 Jenis Perusahaan

Jenis Perusahaan	Jumlah	Presentase
Banking	66	36%
Government	4	2%
Industri dan Trading	10	5%
Service	2	1%
Manufaktur	20	11%
Otomotif	25	14%
Retail Merchandising	38	21%
Securitas	9	5%
Health Care	8	4%

Sumber : data diolah

Berdasarkan tabel 3, dihasilkan jenis perusahaan yang paling banyak adalah *banking* sebesar 36%. Peneliti banyak mengambil populasi pada perbankan, dimana secara umum sistem informasi akuntansi yang diterapkan pada kegiatan operasional perbankan telah terkomputersisasi.

Staff Akuntansi

Kegiatan seorang akuntan yang lebih banyak mengerjakan kegiatan operasional menggunakan perangkat komputer. Data akuntansi dapat dilihat pada tabel 4.

Tabel 4 Jumlah staff akuntansi

Akuntan Profesional	Jumlah	Presentase
50	108	59%
51-100	53	29%
101-150	3	2%
151-200	8	4%
>200	10	6%

Sumber : data diolah

Spesialis Sistem Informasi

Asumsi data bahwa jumlah dari spesialis sistem informasi adalah orang

yang mengerti tentang ancaman dan gangguan sistem. Data spesialis sistem informasi dapat dilihat pada tabel 5

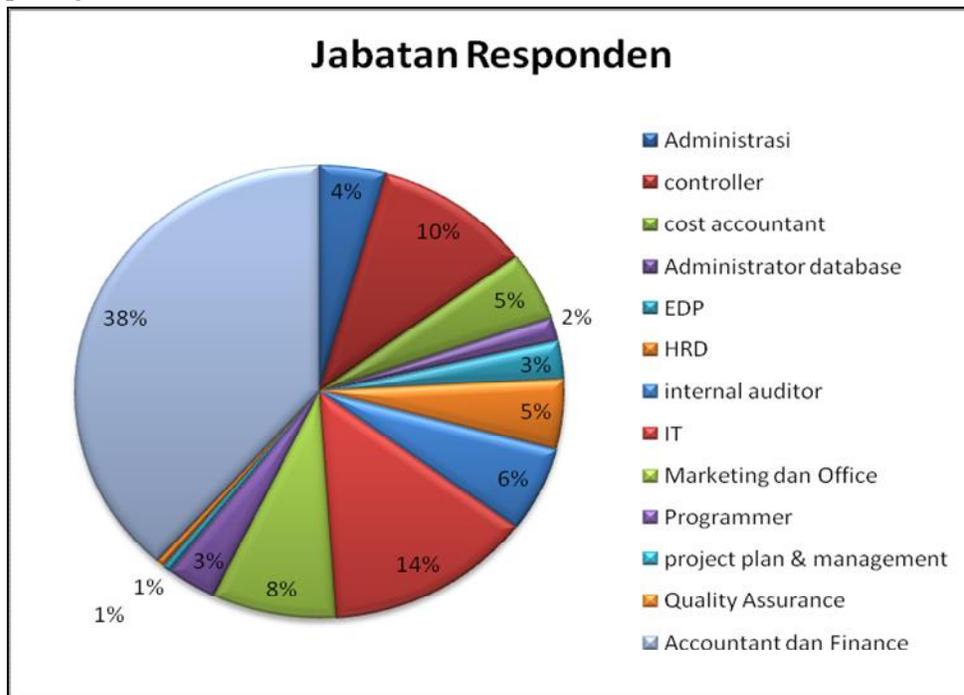
Tabel 5 Jumlah spesialis Sistem Informasi

Spesialis SI	Jumlah	Persentase
5	45	25%
6-10	28	15%
11-15	24	13%
16-20	23	13%
>20	62	34%

Sumber : data diolah

Jabatan responden

Data jabatan responden dapat dilihat pada gambar 1



Gambar 1 Jabatan responden

Frekuensi ancaman keamanan sistem informasi akuntansi

Frekuensi terjadi ancaman keamanan sistem informasi akuntansi dapat dilihat pada tabel 6

Tabel 6. Frekuensi Ancaman

No	Ancaman	Frekuensi				
		1	2	3	4	5
1	Bencana alam seperti banjir, kebakaran, dll	87%	9%	3%	0%	0%
2	Entri data yang buruk di sengaja oleh karyawan	74%	14%	4%	8%	0%
3	Kerusakan data tanpa disengaja oleh karyawan	56%	22%	12%	5%	5%
4	Kerusakan data yang disengaja oleh karyawan	79%	12%	4%	4%	1%
5	Akses tidak sah ke data dan/ atau system oleh karyawan	63%	20%	9%	5%	3%
6	Akses tidak sah ke data dan/ atau system oleh orang luar/ hacker	85%	8%	5%	1%	1%
7	Karyawan berbagi password	33%	20%	13%	9%	25%
8	Bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya SIA	88%	8%	2%	2%	0%
9	Perusakan atau hancurnya output sistem (interupsi)	71%	17%	6%	5%	1%
10	Penciptaan output fiktif/ output salah	75%	13%	8%	4%	0%
11	Pencurian data dan/ atau informasi	79%	13%	5%	2%	1%
12	Menyalin file output tanpa izin	66%	17%	11%	2%	4%
13	Visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak	50%	15%	11%	7%	17%
14	Mencetak file dan di distribusi oleh orang yang tidak berwenang	76%	13%	6%	3%	2%
15	Cetakan dan informasi di arahkan kepada orang yang tidak berwenang	81%	8%	5%	4%	5%
16	Entri data yang buruk tanpa sengaja oleh karyawan	42%	30%	15%	7%	6%
17	Fabrikasi (memasukan pesan palsu, memasukan data palsu, menyerahkan dokumen kepada orang yang tidak di otorisasi)	81%	8%	7%	2%	2%
18	Masuknya virus computer ke system	56%	22%	12%	6%	4%
19	Intersepsi transmisi data dari lokasi jarak jauh	51%	17%	14%	11%	7%

Sumber : Hasil Olah Data

Keterangan tabel :

- 1 : Kurang dari satu tahun sekali
- 2 : Satu tahun untuk bulanan
- 3 : Satu bulan untuk mingguan
- 4 : Satu minggu untuk harian
- 5 : Harian atau lebih sering

Kerugian akibat ancaman keamanan sistem informasi akuntansi

Dari 182 responden tidak semua dapat memberitahukan kerugian akibat gangguan sistem informasi akuntansi. Mereka menyatakan penyebab kerugian akibat gangguan sistem informasi akuntansi banyak di hasilkan dari pihak internal (karyawan) sebesar 66% dan eksternal 34%. Kerugian finansial akibat kesalahan internal berkisar Rp 700.000.000,- sampai Rp 5.000.000.000,- Sedangkan kerugian yang disebabkan dari pihak eksternal berkisar Rp 10.000.000,- sampai Rp 500.000.000,-

Uji Normalitas

Nilai *Asymp Sign* sebesar 0,000 untuk seluruh parameter. Jadi dapat disimpulkan bahwa data pada penelitian ini tidak terdistribusi normal, maka penelitian ini dapat menggunakan uji non parametrik.

Mean Rank

Untuk mengetahui faktor yang paling mengancam keamanan sistem informasi akuntansi dapat dilihat pada tabel 7

Tabel 7 Mean Rank

No	Ancaman	Mean Rank
1	Karyawan berbagi pasword	14.21
2	Bencana alam seperti banjir, kebakaran, dll	12.55
3	Intersepsi transmisi data dari lokasi jarak jauh	12.32
4	Cetakan dan informasi di arahkan kepada orang yang tidak berwenang	12.06
5	Kerusakan data tanpa disengaja oleh karyawan	11.25
6	Penciptaan output fiktif/ output salah	11.18
7	Akses tidak sah ke data dan/ atau sistem oleh karyawan	10.39
8	Mencetak file dan di distribusi kepada orang yang tidak berwenang	10.13
9	Pencurian data dan/ atau informasi	9.49
10	Entri data yang buruk di sengaja oleh karyawan	9.32
11	Menyalin file output tanpa izin	9.20
12	Entri data yang buruk tanpa sengaja oleh karyawan	9.02
13	Fabrikasi (memasukan pesan palsu, memasukan data palsu, menyerahkan dokumen kepada orang yang tidak di otorisasi)	8.72
14	Masuknya virus komputer ke sistem	8.71
15	Kerusakan data yang disengaja oleh karyawan	8.70
16	Visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak	8.57
17	Akses tidak sah ke data dan/ atau sistem oleh orang luar/ hacker	8.24
18	Perusakan atau hancurnya output sistem (interupsi)	7.99
19	Bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya SIA	7.94

Sumber : Output SPSS, diolah

Berdasarkan Tabel 7 dapat dilihat bahwa nilai rata-rata dari perbandingan terhadap jawaban responden mengenai ancaman yang paling mengganggu keamanan sistem informasi akuntansi. Asumsinya adalah semakin besar nilai, semakin sering terjadi, maka semakin mengancam keamanan sistem informasi akuntansi. Berdasarkan informasi pada tabel 7

menyatakan bahwa ancaman yang paling mengganggu adalah parameter karyawan berbagi password.

Uji Beda

Untuk melakukan uji beda, maka peneliti menggunakan uji *Kruskal Wallis*. Hasil uji dapat dilihat pada tabel 8.

Tabel 8 Uji beda dengan *kruskal wallist test*

No	Ancaman	Chi-Square	df	Asymp sign
1	Bencana alam seperti banjir, kebakaran, dll	19.097	8	0.014
2	Entri data yang buruk di sengaja oleh karyawan	11.728	8	0.164
3	Kerusakan data tanpa disengaja oleh karyawan	18.711	8	0.016
4	Kerusakan data yang disengaja oleh karyawan	15.488	8	0.050
5	Akses tidak sah ke data dan/ atau system oleh karyawan	20.903	8	0.007
6	Akses tidak sah ke data dan/ atau system oleh orang luar/ hacker	14.817	8	0.063
7	Karyawan berbagi password	31.743	8	0.000
8	Bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya SIA	33.522	8	0.000
9	Perusakan atau hancurnya output sistem (interupsi)	18.307	8	0.190
10	Penciptaan output fiktif/ output salah	10.634	8	0.223
11	Pencurian data dan/ atau informasi	15.888	8	0.440
12	Menyalin file output tanpa izin	16.167	8	0.400
13	Visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak	22.69	8	0.004
14	Mencetak file dan di distribusi kepada orang yang tidak berwenang	24.537	8	0.002
15	Cetakan dan informasi di arahkan kepada orang yang tidak berwenang	8.309	8	0.404
16	Entri data yang buruk tanpa sengaja oleh karyawan	26.325	8	0.001
17	Fabrikasi (memasukan pesan palsu, memasukan data palsu, menyerahkan dokumen kepada orang yang tidak di otorisasi)	11.610	8	0.169
18	Masuknya virus komputer ke system	18.766	8	0.016
19	Intersepsi transmisi data dari lokasi jarak jauh	29.278	8	0.000

Sumber ; Output SPSS, diolah

Tabel 8 memberikan bukti empiris bahwa ada beberapa ancaman keamanan sistem informasi akuntansi yang berbeda antara entitas perusahaan yaitu bencana alam seperti banjir, kebakaran, dll, kerusakan data tanpa disengaja oleh karyawan, akses tidak sah ke data dan/ atau sistem oleh karyawan, bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya, visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak, mencetak file dan didistribusikan kepada orang yang tidak berwenang, entri data yang buruk tanpa disengaja oleh karyawan, masuknya virus komputer ke sistem, dan intersepsi transisi data dari lokasi jarak jauh.

Hal tersebut disebabkan nilai signifikansi (Asymp. Sig < 0,05). Hal ini didukung dengan penelitian Yulius kurnia dan Ratih Handayani (2008) terdapat perbedaan pada masuknya virus ke komputer sistem dan Abu Musa (2006).

KESIMPULAN

Berdasarkan hasil survei penelitian, menyatakan bahwa ancaman keamanan yang paling mengganggu sistem informasi akuntansi adalah karyawan berbagi password dan terdapat perbedaan antara berbagai jenis perusahaan mengenai ancaman keamanan sistem informasi yaitu bencana alam seperti banjir, kebakaran, dll, kerusakan data tanpa disengaja oleh karyawan, akses tidak sah ke data dan/ atau sistem oleh karyawan, bencana yang dibuat manusia seperti kebakaran, kehilangan sumber daya, visibilitas dokumen sah dengan menampilkan pada monitor atau dicetak, mencetak file dan didistribusikan kepada orang yang tidak berwenang, entri data yang buruk tanpa disengaja oleh karyawan, masuknya virus komputer ke sistem, dan intersepsi transisi data dari lokasi jarak jauh.

SARAN

Berdasarkan hasil penelitian, maka peneliti memberikan saran untuk penelitian selanjutnya untuk memperluas dan meningkatkan penelitian ini dalam menyelidiki ancaman keamanan sistem informasi akuntansi, meneliti pengaruh ancaman keamanan sistem informasi terhadap kegiatan operasional perusahaan dan menambah area populasi sampel.

DAFTAR PUSTAKA

- Dasaratha V Rama, Frederick L Jones. Edisi 18 buku 1. 2008. *Sistem Informasi Akuntansi*. Salemba Empat
- Krismiaji. 2010. Edisi Ketiga. *Sistem Informasi Akuntansi*. UPP STIM YKPN : Yogyakarta
- Kadir, Abdul. Edisi Revisi. 2014. *Pengenalan Sistem Informasi*. Andi, Yogyakarta
- Romney, B. Marshall and Steinbart, Paul. 2012. *Accounting Information Systems*. Global Edition. 12 th edition. England: Pearson Education Limited.
- Abu-Musa, Ahmad A. 2004. Exploring the Perceived Threats of Computerized Accounting Information System in Emerging Countries: an Empirical Study on Saudi Organization. *European Accounting Information Systems Conference*. Prague : Annual Congress of the European Accounting Association
- Abu-Musa. Ahmad A. 2006. Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations. *King Saud Univ, Vol. 18, Comp. & Info. Sci., pp. 1-26*.