Identifikasi Risiko Sistem Informasi Teknologi pada Perguruan Tinggi

Jaqolina Anggraeni Vigim[1], Nugraha[2], Alfira Sofia[3], R. Nelly Nur Apandi[4], Budi Purnomo[5]
Magister Ilmu Akuntansi, Sekolah Pascasarjana, Universitas Pendidikan Indonesia, Bandung, Indonesia[1]
Program Studi Akuntansi, FPEB, Universitas Pendidikan Indonesia, Bandung, Indonesia[2]
Program Studi Akuntansi, FPEB, Universitas Pendidikan Indonesia, Bandung, Indonesia[3]
Program Studi Akuntansi, FPEB, Universitas Pendidikan Indonesia, Bandung, Indonesia[4]
Program Studi Akuntansi, FPEB, Universitas Pendidikan Indonesia, Bandung, Indonesia[5]

Abstract

Implementing information technology systems (SIT) in universities makes it easier to communicate, but SIT also causes abuse called *cybercrime*. Information technology systems (SIT) are almost used by all universities but are not followed by understanding the negative impacts of using SIT. This study aims to identify the risk of SIT in universities. Risk identification is carried out by conducting interviews with SIT experts and audit experts. The results of this study are that there are 19 risks identified and grouped into 3 (three), namely financial, academic and operational risks. This risk identification can be used as a guideline for higher education internal audits in finding the scope and audit evidence.

Keyword: analysis; control; *cybercrime* ; evaluation; identification risk; technology information system; university.

Abstrak

Implementasi sistem informasi teknologi (SIT) pada perguruan tinggi memudahkan dalam berkomunikasi namun SIT juga menimbulkan penyalahgunaaan yang disebut *cybercrime.* Sistem informasi teknologi (SIT) hampir digunakan oleh seluruh perguruan tinggi, namun tidak diikuti dengan pemahaman mengenai dampak negatif dari penggunaan SIT tersebut. Penelitian ini bertujuan untuk melakukan identifikasi risiko SIT pada perguruan tinggi. Identifkasi risiko dilakukan dengan melakukan wawancara kepada ahli SIT dan ahli audit. Hasil penelitian ini yaitu terdapat 19 risiko yang teridentifikasi dan dikelompokkan menjadi 3 (tiga) yaitu risiko keuangan, akademik dan operasional. Identifikasi risiko ini dapat menjadi pedoman bagi audit internal perguruan tinggi dalam mencari cakupan ruang lingkup dan bukti audit.

Kata Kunci: analisis; *cybercrime;* identifkasi; pengendalian; penilaian; perguruan tinggi; risiko; sistem informasi teknologi.

Corresponding author. jaqolinaaa@student.upi.edu[1], nugraha@upi.edu[2].
Alfira.sofia@upi.edu[3],nelly.nna@upi.edu[4], budi.purnomo@upi.edu[5]

History of article. Received: April 2021, Revision: Juni 2021, Published: September 2021

PENDAHULUAN

Penyampaian informasi dan cara berkomunikasi seiring dengan perkembangan teknologi berubah menjadi digital atau dinamakan digitalisasi ekonomi (The digital economy, 2015). Dalam memproduksi, mengolah dan menyebarkan informasi, pada awalnya masyarakat menggunakan metode tatap muka sebagai sarana penyampaian informasi. Seiring dengan kemajuan teknologi, media massa dan peralatan teknologi lainnya muncul sebagai pengganti metode tatap muka untuk memudahkan masyarakat dalam menyebarluaskan informasi. Dengan adanya media massa dan peralatan teknologi lainnya, maka proses penyebaran informasi menjadi berkembang dan berubah dari format analog menjadi format digital.

Perkembangan sistem teknologi informasi (SIT) digunakan dalam berbagai bidang tanpa batasan jarak yang dinamakan *cyberspace* (Sanusi, 2005). Masuknya cyber space berdampak pada berbagai bidang manusia dari berbagai aspek sosial, ekonomi, politik dan hukum (Makarim, 2005). Adanya penggunaan internet dan SIT memberikan

dampak positif yaitu memudahkan dalam berkomunikasi dan bertransaksi.

Dalam melakukan komunikasi yang tidak terbatas pada jarak maka dapat menimbulkan kesalahpahaman dikarenakan perbedaan kultur sosial. Siegel (1989) menjelaskan, bahwa teori asosiasi diferensial mengkaji tentang elemen-elemen dalam masyarakat yang berpengaruh terhadap seseorang yang melakukan perbuatan jahat (Indah Nurfitria, Maroni, 2013). Adanya kejahatan dan perbedaan tujuan ini melalui proses interaksi dan komunikasi. Perbuatan jahat atau penyalahgunaan komunikasi inilah yang dapat menimbulkan risiko penggunaan SIT.

Dampak negatif seperti adanya penyalahgunaan SIT dinamakan *cybercrime* (Moore, 2010). *Cybercrime* ini dapat terjadi di beberapa bidang diantaranya bisnis publik dan swasta, organisasi nirlaba, lembaga pendidikan, dan lembaga pemerintah (Moore, 2010).

Berdasarkan jenis *cybercrime* pada Redaksi (2016), jenis *cybercrime* tersebut memiliki potensial untuk terjadi di institusi pendidikan, diantaranya: *Unauthorized Access to Computer System and technology, Illegal Contents, Data forgency, Cyber Espionage, Cyber Sabotage and Extortion, Offense against Intellectual Property, Infringements of Privacy*. Perkembangan *cybercrime* ini terjadi di beberapa bidang seperti bisnis publik dan swasta, organisasi nirlaba, lembaga pendidikan, dan lembaga pemerintah (Moore, 2010).

Cybercrime di bidang pendidikan dapat terjadi seperti adanya sewa jasa hacker untuk meretas akun penilaian, gaji, kinerja pegawai, penyalahgunaan aset, provokasi dan lainnya. Penggunaan SIT di perguruan tinggi tidak diikuti dengan pengetahuan mengenai dampak penyalahgunaannya. Toma et al. (2014) menyatakan bahwa risiko yang terjadi di bidang akademi memiliki tingkat risiko lebih tinggi dibandingkan dengan bidang lainnya seperti bank, organisasi non profit dan pemerintahan.

Adanya potensi *cybercrime* merupakan ancaman yang dapat memunculkan risiko bagi perguruan tinggi. Maka audit internal selaku manajemen oragnisasi yang memiliki peran dan fungsi membantu perguruan tinggi dalam mencapai tujuan yang telah ditetapkan dengan melakukan perbaikan proses, penguatan sistem pengendalian internal dan meningkatkan efektivitas manajemen resiko (Permana, 2020, Soobaroyen et al., 2018).

Manajemen risiko menurut Whitman & Mattord (2010:277) adalah proses yang berupa perlindungan dan kontrol yang diimplementasikan. Menurut Djohanputro (2008:43) manajemen risiko adalah proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan dan memonitor alternatif penanganan risiko, dan mengendalikan implementasi penanganan risiko. Menurut Toma et al. (2014), terdapat empat risiko yang diidentifikasi dan dianalisis yaitu risiko akademik, keuangan, strategis dan operasional.

Pada perguruan tinggi audit internal selaku manajemen organisasi. Salah satu ruang lingkup audit internal yaitu dengan melakukan penilaian atas pengendalian internal (Sawyer, 2009). Dalam mencapai tujuan organisasi, maka audit internal perlu melakukan penilaian atas pengendalian internal dengan melakukan penilaian risiko

Menurut Hollman & Mohammad-Zadeh (1984) terdapat beberapa langkah untuk mengimplementasikan manajemen risiko, diantaranya identifikasi risiko, analisis risiko, pemilihan teknik, penerapan strategi, dan pengendalian. Dalam penelitian ini berfokus pada identifikasi risiko SIT pada perguruan tinggi.

Terdapat beberapa metode pengumpulan informasi yang dapat digunakan untuk mengidentifikasi risiko. Tetapi ada tiga metode yang paling sering digunakan yaitu

brainstorming (bertukar pikiran) dalam teknik ini para ahli bertukar pikiran mengenai sumber risiko yang mungkin terjadi; *Risk Breakdown Structure (RBS)* dengan melakukan penyusunan risiko berdasarkan kategori tertentu (Susilo & Kaho, 2014); analisis SWOT yang digunakan untuk menetapkan kemungkinan risiko, tahap ini juga dapat digunakan dalam sesi *brainstorming*.

Berdasarkan pemaparan terkait adanya risiko SIT, maka penelitian ini mengeksplorasi berbagai jenis risiko yang mungkin timbul dari penggunaan SIT pada perguruan tinggi. Hasil dari penelitian ini memberikan kontribusi dalam proses identifikasi risiko sehingga perguruan tinggi dapat melakukan tindakan *preventif* terhadap risiko yang timbul.

METODE

Objek penelitian variabel yang diteliti oleh peneliti ditempat penelitian dilakukan. Maka objek penelitian ini adalah benda, orang ataupun tempat yang menjadi suatu dan sasaran penelitian (Supriyati, 2012). Berdasarkan penjelasan di atas dalam penelitian ini yang menjadi objek penelitian adalah risiko sistem informasi teknologi di perguruan tinggi.

Desain penelitian pada penelitian ini adalah kualitatif, yaitu data berupa kata-kata, gambar, dan bukan angka (Danim, 2002). Pendekatan penelitian menggunakan pendekatan fenomenologi, yang berfokus kepada pengalaman nyata untuk menggambarkan pengalaman (Patton, 1990).

Pengambilan data kepada stakeholder perguruan tinggi sebagai populasi dan sampel diambil dengan teknik *purposive sampling* dengan kriteria informan memiliki pengalaman atau ahli dalam penggunaan SIT dan risiko. Setelah itu dilakukan teknik pengambilan *snawballing sampling*.

Metode penelitian ini menggunakan desain penelitian kualitatif dengan pendekatan fenomenologis. Data yang digunakan yaitu data primer dari hasil wawancara, kuesioner dan observasi. Sampel nya yaitu ahli audit dan ahli SIT.

Teknik pengumpulan data dengan melakukan wawancara dan observasi. Wawancara kepada ahli audit dan SIT, sedangkan observasi dengan melakukan pengamatan di media sosial.

HASIL DAN PEMBAHASAN

Hasil pengumpulan data responden menyatakan bahwa risiko SIT pada perguruan tinggi sebagai berikut:

Responden satu, hal utama yang harus dijaga itu kerahasiaan data, integritas informasi dan data maksudnya sistem teknologi informasi ini mampu menjaga keakuratan dan keaslian ketika dibutuhkan kredibilitasnya terjamin. Sistem teknologi informasi harus bisa menjamin keamanan data user ketika user menggunakan sistem teknologi informasi tersebut dan juga harus menyediakan informasi yang dibutuhkan (*availability*).

Bentuk ancaman untuk risiko penggunaan sistem teknologi informasi selain faktor natural atau faktor alam/bencana (mati listrik, bencana, *force majeure*) yaitu ancaman muncul dari hacker atau orang ketiga yang punya kemampuan dan skill dalam melakukan peretasan terhadap sistem informasi teknologi, proses hacker ini belum sampai tahap merusak sistem informasi teknologi, apabila sampai merusak maka disebut *cracker*. Ada juga ancaman social engineering, si hacker ini melakukan gangguan kepada user terlebih dahulu seperti melakukan penipuan melalui pesan SMS atau telpon palsu, email (*spoofing*) dengan mengatasnamakan pejabat atau stakeholder kampus apabila di lingkup perguruan tinggi. Serangan ini dilakukan dengan cara clickbait.

Fenomena penggunaan sistem teknologi informasi di perguruan tinggi seperti: penggunaan sistem nilai yang menggunakan sistem teknologi informasi, hacker dapat meretas sistem tersebut untuk merubah nilai atau melakukan serangan terhadap security

system yang lemah. Penggunaan sistem presensi, dengan adanya kemampuan atau skill sistem teknologi informasi, maka user bisa membuat BOT untuk auto isi presensi dan auto login.

Dari sisi presensi dosen atau tenaga kependidikan terdapat celah seperti social engineering untuk menduplikasi finger print/face recognition, dari segi keamanan device juga memungkinkan adanya celah hacker (*Internet of Thinking Attack*), dari segi jaringan yang terkoneksi ke sistem untuk mencatat transaksi yang sudah ada hal ini terdapat celah seperti menambahkan jaringan untuk menambahkan presensi hadir padahal orang yang bersangkutan tidak hadir, dari segi software terdapat celah masuk dari jaringan seperti dimasukkan virus untuk meretas. Penggunaan sistem pembayaran UKT adanya sistem yang terintegrasi antara kampus dengan pihak bank, biasanya terdapat jalur komunikasi, dari jalur komunikasi ini bisa diretas oleh pihak ketiga, seperti bisanya dilakukan perubahan status bayar dan perubahan nominal.

Apabila hacker sudah ditahap modifikasi seperti menambahkan, mengurangi, menghapus dll dalam artian mengambil hak istimewa atau mengambil alih fungsi admin bahkan sampai bisa melakukan pabrikasi dalam artian menyisipkan hal-hal yang bisa menjadi media hack atau iklan bahkan bisa menyisipkan hal negatif, hacker bisa menjadikan sistem teknologi informasi menjadi media untuk menyisipkan virus untuk melakukan perusakan. Seperti adanya pengumuman yang dilakukan via email oleh *official account* kampus atau email kampus kepada seluruh stakeholder dengan menyisipkan url atau link website yang didalamnya sudah terdapat virus untuk mengambil data pribadi mahasiswa atau stakeholder.

Responden kedua, risiko itu banyak, kalau berdasarkan pengalaman yaitu risiko data dan risiko SDM. Jadi ketika menerapkan sistem teknologi informasi di entitas, SDM nya perlu mengetahui cara pemakaiannya. Kalau masalah risiko data, sistem teknologi informasi tidak sistem yang 100% aman maka perlu dilakukan maintenance.

Risiko potensi hacker tergantung ke sistemnya, semua sistem teknologi informasi memiliki potensi untuk di hack tergantung manfaat dan keuntungan bagi hacker. Berdasarkan pengalaman pernah terjadi peretasan sistem teknologi informasi dengan tujuan merubah nilai. Pemanfaatan sistem teknologi informasi dikampus tidak hanya data saja, ada juga pemanfaatan jaringan wifi, dalam artian orang yang tidak memiliki haknya untuk menggunakan wifi di wilayah perguruan tinggi melakukan peretasan dengan memanfaatkan fasilitas tersebut. Jika hal ini terjadi terus menerus dan berjangka panjang maka akan menimbulkan kerugian bagi pihak kampus dalam membayar tagihan wifi atau jaringan tersebut. Penggunaan sistem informasi di perpustakaan untuk jurnal berbayar juga dapat dilakukan peretasan dengan menggunakan manfaat dari akses gratis tersebut.

Peretasan informasi keuangan merupakan hal yang krusial, informasi keuangan mencerminkan sehat dan tidaknya suatu entitas, dan menggambarkan suatu transaksi dari berbagai pihak. Misalnya mahasiswa A mampu bayar 13,5jt per semester hal ini bisa dimanfaatkan oleh hacker untuk mapping dalam artian mengelompokkan jenis mahasiswa. Terdapat informasi berapa besaran mendapatkan insentif dari pemerintah untuk membuat kelompok universitas. Hal ini bisa dimanfaatkan oleh hacker untuk menargetkan kejahatan.

Pengalaman pribadi responden terkait pencurian data lewat kampus, pihak ketiga mengetahui data pribadi mahasiswa untuk melakukan penipuan dengan menghubungi orang tua nya. Dengan data-data valid yang dimiliki oleh hacker, menjadikan orangtua mahasiswa tersebut mengalami penipuan. Meskipun hal ini tidak terjadi, namun hal ini

mencerminkan kalau data kampus sudah bocor.

Fenomena lain syarat salah satu universitas untuk *cumlaude* yaitu dengan publish jurnal, namun karena adanya proses yang sulit memungkinkan untuk melakukan website dummy atau pembuatan link palsu (*phising*). Hal ini tergantung SOP kampus tersebut, apabila SOP nya sudah betul maka untuk melakukan hal tersebut kemungkinan terjadinya kecil, dan sebaliknya.

Dalam sistem pendaftaran mahasiswa, memungkinkan adanya peretasan perubahan status menjadi lulus dan perubahan golongan UKT, hal ini terjadi apabila tidak dilakukannya validasi dan SOP yang ada. Adanya risiko dari pihak internal seperti memungkinkan tagihan mahasiswa 10jt, oleh adm kampus di up di sistem menjadi 12jt, 2jt tersebut tidak dilaporkan menjadi pencapatan universitas. Celah di sistem keuangan lebih tinggi daripada sistem administrasi.

Ada beberapa kampus yang tidak memperbolehkan penyimpanan data diluar indonesia, hal ini mempertimbangkan risiko yang diperoleh apabila mempercayakan data kepada pihak pengelola. Jika dikelola sendiri maka risiko hanya ditanggung oleh sendiri, tidak melibatkan pihak ketiga.

Risiko ketika sistem informasi down, ketika melakukan ujian online yang dilaksanakan oleh pihak kampus karena banyaknya orang yang akses maka sistem down hal ini mengganggu kegiatan belajar mengajar. Harusnya pihak IT mampu mengestimasi berapa jumlah mahasiswa, dosen dan staff yang mengakses sistem tersebut. Fenomena ini terjadi disalah satu kampus. Selain itu dalam penginputan nilai oleh dosen, apabila *server down* dan dosen tidak menyampaikan nilai tepat waktu maka terjadi pengurangan gaji (tergantung kebijakan universitas).

Dalam proses pendaftaran jika tanpa SOP dan validasi, ketika melampirkan data seperti transkrip data dilakukan perubahan nilai menggunakan aplikasi edit foto (pemalsuan data) lalu di upload ke laman pendaftaran. Manipulasi data bisa terjadi dua arah misal eksternal yaitu mahasiswa mengedit data untuk di upload, dan internal yaitu misalnya ada kerabat kerja di bagian penerimaan mehasiswa, lalu melakukan penggantian data dan juga menyewa pihak ketiga utnuk melakukan perubahan data.

Responden ketiga, adanya perkuliahan daring dan kegiatan kampus menjadi digital memungkinkan timbulnya risiko, risiko seperti jual beli nilai, kebocoran data, remunerasi, website di hack, perubahan jam pengumpulan tugas, kelulusan yang direkayasa, keringanan UKT yang tidak sesuai dengan ketentuan, status pajak yang dirubah, penyalahgunaan website, rekayasa hasil penelitian.

Diantara beberapa risiko tersebut berdasarkan pengalaman dan paling jelas yaitu jual beli nilai karena sering terjadi, baik secara digital maupun manual. Misalnya ada orang yang pinter dibidang IT, dia bisa melakukan peretasan, hal ini dengan beberapa pertimbangan seperti tidak mau mengulang mata kuliah tersebut atau tidak mau membayar UKT lanjutan. Di salah satu kampus swasta, mahasiswa A mendapat nilai E lalu meminta pihak ketiga untuk melakukan perubahan, untuk kejadian ini apabila kampus tidak bisa melakukan trashback maka peretas dan mahasiswa tersebut tidak mendapatkan hukuman apapun.

Lalu yang kedua yang paling umum yaitu adanya kebocoran data, kampus memiliki data-data mahasiswa, dosen dan staff lainnya. Kasus simple seperti bocornya data no handphone, untuk melakukan penipuan dengan mengaku salah satu pejabat kampus untuk melakukan penipuan terhadap mahasiswa. Dari adanya kebocoran data ini, stakeholder akan mengalami kerugian karena hacker atau perertas bisa melakukan penargetan terhadap stakeholder. Kebocoran data lainnya seperti kebocoran soal ujian seleksi penerimaan mahasiswa, hal ini juga dapat menjadi kerugian bagi universitas.

Yang ketiga yaitu perubahan tampilan di website, misalnya ada kejadian perlakuan

kampus yang tidak disenangi oleh mahasiswa atau salah satu pihak maka dilakukan peretasan. Hal ini menghambat aktivitas divisi terkait, dan ketersediaan informasi menjadi terhambat. Bisa juga terjadi penyisipan virus ke salah satu file, misalnya menyisipkan di data panduan penyusunan karya ilmiah, ketika mahasiswa mengdownload maka virus nya juga ikut terbawa.

Yang keempat yaitu waktu pengumpulan tugas. Adanya kemungkinan melakukan perubahan terhadap perpanjangan waktu pengumpulan tugas. Tanpa adanya peretasan pun jika waktunya sudah habis, kadang mahasiswa masih bisa mengupload. Apabila ada mahasiswa yang memiliki skill IT untuk melakukan perubahan atas waktu pengumpulan tanpa adanya erorr dari website tersebut. Misalnya pada awalnya di set 10 jam dengan dibuat bot maka diubah menjadi 11 jam.

Yang kelima, kelulusan direkayasa misalnya mahasiswa yang kuliah di universitas tertentu tapi mengikuti proses pengajaran, jadi melakukan perubahan atas status kemahasiswaan mahasiswa tersebut. Oleh karena itu proses validasi atau verifikasi masih diperlukan.

Yang keenam dari sisi keuangan, tidak menutup kemungkinan untuk melakukan peretasan perubahan jumlah nominal pembayaran UKT. Hal ini bisa dilakukan peretasan atas data base yang dimiliki universitas. Misalnya di database UKT nya 5jt, maka dirubah menjadi lebih kecil atau merubah status bayar.

Yang ketujuh, melakukan rekayasa terhadap hasil jurnal dalam mengikuti lomba. Dalam prosesnya terdapat prosiding, bisa jadi ada celah bagi hacker dalam melakukan fraud untuk mempermulus proses lomba atau kompetisi, bisa juga merubah data asalnya tidak lulus menjadi lulus publish. Risiko lain yang mungkin timbul yaitu website dummy dengan membuat tampilan yang sama seolah-olah sudah terpublish.

Responden keempat, risiko yang mungkin timbul dari penggunaan IT seperti dari penggunaan wifi atau jaringan, seperti adanya pencurian data. Risiko lainnya seperti melakukan peretasan untuk merubah nilai oleh mahasiswa, *cybertech* dengan melakukan hacker ke jaringan seperti menjadikan server down, perubahan data. *Cybertech* ini sering terjadi di salah satu kampus. Selain itu ada pencurian data dan jual beli data, lalu mempelajari data base untuk dijadikan dasar dalam melakukan penipuan.

Pencurian asset melalui device dimana file nya belum di publish seperti pencurian data dari device PC atau laptop dosen atau pejabat terkait. Misalnya meretas basis data PC divisi keuangan untuk melihat anggaran, meretas laptop dosen untuk mencuri data soal ujian dan kunci jawabannya.

Lalu penyadapan terhadap data yang sedang dikumpulkan, misalnya dalam penyebaran kuesioner atau google form data pribadi tiba-tiba ada pihak ketiga yang melakukan penyadapan atas data tersebut untuk kepentingan pribadi. Secara garis besar risiko-risiko yang mungkin timbul itu seperti pencurian data pribadi, pencurian aset berharga, dan perubahan data berharga.

Adanya kehilangan dokumen atau file yang sudah terupload di sistem informasi, misalnya mahasiswa sudah upload tugas di sistem informasi, akan tetapi di sistem dosen tidak terdeteksi untuk file tersebut. Hal tersebut bisa dijadikan risiko yang mungkin menjadikan miss komunikasi antara dua pihak.

Responden kelima, terkait adanya kewajiban publish jurnal untuk penelitian, memungkinkan adanya pembuatan website dummy seolah-olah sudah melakukan submit jurnal padahal tidak sama sekali. Namun hal ini kembali ke SDM perguruan tinggi tersebut dalam menvalidasi untuk hal pengajuan dana penelitian tersebut.

Responden keenam, celah terjadinya risiko, yaitu tidak terupdatenya sistem. Selain karena human erorr karena sistem nya dari

pemerintah sudah aman, kalau terkait otoritasi memungkinkan adanya penyalahgunaan. Karena adanya penyalahgunaan otorisasi memungkinkan adanya pencurian aset atau uang.

Responden ketujuh, terdapat 4 point risiko penggunaan teknologi informasi, yang pertama mengenai hacker atau adanya peretasan sistem, kalau dari website sering sekali adanya peretasan. Yang kedua, mengenai teknis risiko nya terkait dengan masalah ketersediaan tempat penyimpanan, Yang ketiga, mengenai jaringan, biasanya dirasakan oleh kampus-kampus di luar kampus utama, mereka mengalami hambatan dalam menggunakan aktivitas berbasis web. Yang keempat, risiko pemeliharaan jaringan atau konektor sendiri, misalnya gedung A mengalami hambatan dalam penggunaan internet, hal ini mengakibatkan SIT di gedung A menjadi terhambat.

Responden kedelapan, perguruan tinggi membuat laporan keuangan dimana terdapat peran IT environtment, IT environtment bisa dimanipulasi bisa wewenang terentu mengakses sampai ke proses programing, IT ini bisa mengkontrol laporan keuangan untuk salahsaji agar laporan keuangan nya itu bagus dan terlihat kuat.

Responden kesembilan, risiko jual beli Nilai : lemahnya sistem IT ialah jual beli nilai mahasiswa. Resiko ini sangat mungkin terjadi dimana data sistem penilaian mahasiswa dapat diretas melalui pihak ketiga. Tidak hanya itu, jika sistem IT lemah dan tidak memiliki keamanan ganda, maka dapat disalahgunakan; kebocoran data : data yang dikolektif oleh pihak kampus mengenai data pribadi mahasiswa mungkin dapat diretas oleh pihak ketiga dengan tujuan tertentu. – pinjaman online; hacker website : peretasan website kampus, hal ini menghambat kinerja divisi terkait. Dimana tidak dapat melakukan kegiatan berbasis website. Seperti halnya terdapat penjadwalan pemberian informasi oleh pihak universitas kepada mahasiswa, namun karena adanya serverdown atau peretasan website maka hal itu tidak dapat dilakukan; rekayasa/manipulasi data untuk menguntungkan pihak tertentu; remunerasi : di beberapa universitas untuk data absensi setiap harinya sudah menggunakan finger print dan scan wajah. Dalam penggunaan IT absensi ini, untuk absensi tidak hadir yang seharusnya tidak digaji maka bisa jadi dirubah untuk alasan tertentu; informasi mengenai piutang : pihak perguruan tinggi memiliki informasi mengenai utang piutang antara mahasiswa dengan pihak kampus, hal ini memungkinkan timbulnya risiko peretasan dan perubahan data mengenai utang piutang. Mahasiswa mungkin bisa melakukan peretasan dengan merubah status bayar atau nominal bayar yang tertera pada sistem dan merubah basis data yang dimiliki oleh perguruan tinggi; pengumpulan tugas yang tidak tepat waktu: risiko mahasiswa melakukan perubahan jam pada submit tugas mungkin dapat terjadi. Mahasiswa dengan keahlian khusus untuk meretas system atau bahkan menyewa pihak ketiga dalam melakukan hal tersebut; kelulusan yang direkayasa: Seolah-olah merupakan lulusan universitas A namun kenyataannya tidak menjadi mahasiswa A, bisa juga sudah menjadi mahasiswa kampus A namun tidak lulus, sedangkan data di sistem informasi menunjukkan bahwa orang tersebut merupakan alumni kampus A; keringanan UKT: misal dalam penggolongan pembayaran UKT, mahasiswa A mendapat golongan 2 dengan jumlah yang harus dibayar 10jt, namun karena orang tersebut tidak menerima maka melakukan peretasan dengan mengubah data tersebut menjadi golongan 4 dengan jumlah bayar 5jt. Selain itu mengenai pemberian keringanan UKT, memungkinkan adanya celah untuk melakukan fraud dengan cara memanipulasi data agar terlihat tidak mampu sehingga lolos adm, atau bisa juga tidak lolos secara adm namun mampu merubah sistem menjadi diberi keringanan 50%; rekayasa hasil akurasi penelitian : adanya tindakan peretasan dengan cara merubah data penilaian tersebut agar hasil penelitian lolos dan terlihat bagus;

rekayasa/manipulasi link website; penyalahgunaan website jurnal penerbit: adanya manipulasi link website sehingga seolah-olah jurnal tersebut sudah submit di jurnal yang memenuhi standar namun pada kenyataannya tidak publish sama sekali.

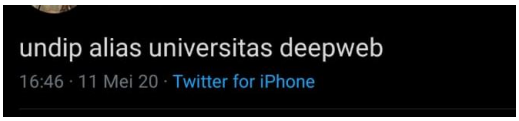
Gambar 1. *Word cloud*

Tabel 1. *Count Word cloud*

Word	Count	Word	Count
Data	76	excel	8
System	76	tugas	8
Informasi	51	diretas	6
Risiko	46	meretas	6
Teknologi	31	publish	6
Keuangan	24	virus	6
Peretasan	22	kerugian	5
Hacker	20	manipulasi	5
Penggunaan	20	pengumpulan	5
Perubahan	18	presensi	5
Website	17	wifi	5
Laporan	16	absensi	4
Nilai	15	dirubah	4
Pencurian	15	link	4
Jaringan	13	lulus	4
Universitas	13	menyisipkan	4
Penyalahgunaan	11	nominal	4
Ukt	11	pajak	4
Dosen	10	piutang	4
Merubah	10	dummy	3
Celah	9	Finger	3
Jurnal	9	Fraud	3
		penyadapan	3

Sumber: data diolah, Nvivo 2021

Hasil deskripsi dari 9 responden dibuat wordcloud untuk mengetahui kata kunci untuk mengidentifikasi risiko, sebagai berikut:

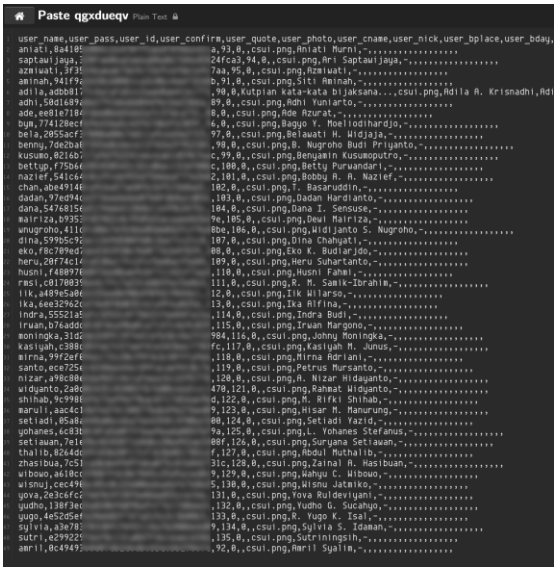


Gambar 2. *Hate spee*

Selain dilakukan wawancara juga dilakukan observasi, observasi dilakukan dengan memantau sosial media twitter dan website sehingga mendapatkan hasil sebagai berikut:

Gambar 2. Peretasan website

Gambar 3. Peretasan website



Gambar 4. Pencurian data

Dari dua teknik pengambilan data tersebut, maka teridentifikasi 19 risiko yang dikelompokkan menjadi 3 (tiga). Pertama, risiko akademis seperti perubahan waktu dalam pengumpulan tugas, penggantian nilai mahasiswa melalui peretasan sistem, kelulusan yang direkayasa. Kedua, risiko sumber daya manusia untuk risiko stategis dan operasional seperti penggantian status pajak untuk mengurangi beban pajak pribadi melalui peretasan sistem, peretasan device dosen untuk dicuri data ujian, penggantian data absensi finger print mahasiswa, dosen, staff dan tenaga kependidikan, penyalahgunaan website jurnal penerbit seperti membuat website dummy, penggunaan BOT untuk auto login dan auto isi presensi, penyisipan BOT untuk membuat server down, rekayasa hasil akurasi kelayakan penelitian, manipulasi data yang akan di upload, peretasan dan penyalahgunaan website dan sosial media dengan menyisipkan hate speech mengenai perguruan tinggi atau stakeholder, social engineering, spoofing data dan kebocoran data stakeholder untuk melakukan penipuan dan kejahatan lainnya, penyisipan virus ke dokumen dan disebarkan melalui website dan email resmi, penyadapan rapat resmi atau informasi resmi (*Men in Middle*), pemanfaatan fasilitas wifi atau fasilitas berbayar lainnya diluar perguruan tinggi. Ketiga, risiko keuangan diantaranya penggantian data mengenai transaksi piutang mahasiswa, peretasan jalur komunikasi sistem informasi antara bank dan perguruan tinggi untuk transaksi keluar masuk uang, server crack untuk menghapus data transaksi keuangan.

KESIMPULAN

Penilaian risiko terdiri dari tiga tahap yaitu identifikasi, analisis dan pengendalian. Identifikasi risiko *cybercrime* di perguruan tinggi terdapat 19 risiko yang dikelompokkan menjadi risiko keuangan, akademik dan SDM.

Saran untuk penelitian selanjutnya berfokus pada satu perguruan tinggi; melakukan penelitian lanjutan untuk tahap analisis dan pengendalian risiko; melakukan rangkaian komprehensif sesuai ISO 31000 ; dan melakukan validasi dengan cara FGD (*forum group disscusion)*.

DAFTAR PUSTAKA

Danim, S. (2002). *Menjadi Peneliti Kualitatif Rancangan Metodologi, Presentasi, dan Publikasi Hasil Penelitian untuk Mahasiswa dan Penelitian Pemula Bidang Ilmu Sosial, Pendidikan, dan Humaniora* (Cetakan 1). Remaja Rosdakarya.

Hollman, K. W., & Mohammad-Zadeh, S. (1984). Risk management in small business. *Journal of Small Business Management*.

Indah Nurfitria, Maroni, R. F. (2013). Analisis Kriminologis Terhadap Tindak Pidana Korupsi Penyalahgunaan Wewenang Dalam Jabatan Pemerintahan Di Bandar Lampung. *POENALE : Jurnal Bagian Hukum Pidana*. https://doi.org/10.1017/CBO9781107415324.004

Makarim, E. (2005). *Pengantar Hukum Telematika*. Grafindo Persada.

Moore, J. W. (2010). From Phishing To

Advanced Persistent Threats: The Application Of *Cybercrime* Risk To The Enterprise Risk Management Model. *Review of Business Information Systems (RBIS)*, *14*(4), 27–36. https://doi.org/10.19030/rbis.v14i4.358

Patton. (1990). *Qualitative Evaluation and Research Methods* (Vol.1). Sage Psikologi Sosial.

Permana, A. (2020). *Audit Internal Berperan Penting dalam Tata Kelola Perguruan Tinggi*. https://www.itb.ac.id/berita/detail/57487/audit-internal-berperan-penting-dalam-tata-kelola-perguruan-tinggi

Redaksi. (2016). *Jenis Cybercrime Berdasarkan Motif dan Aktivitasnya*. Jurnal Security. https://jurnalsecurity.com/jenis-modus-operandi-*cybercrime*/

Sanusi, M. A. (2005). *Hukum Teknologi dan Informasi*. Tim Kemas Buku.

Sawyer, L. B. (2009). *Internal Auditing* (Edisi lima). Salemba Empat.

Siegel, L. J. (1989). *Criminologigy* (third edit). West Publishing Company.

Soobaroyen, T., Ntim, C. G., Broad, M. J., Agrizzi, D., & Vithana, K. (2018). Exploring the oversight of risk management in UK higher education institutions: The case of audit committees. *Accounting Forum*, *October 2017*, 0–1. https://doi.org/10.1016/j.accfor.2018.09.003

Supriyati. (2012). *Metode Penelitian*. Labkat press UNIKOM.

Susilo;, L., & Kaho, V. R. (2014). *Manajemen Risiko Berbasis ISO 31000 untuk Industri NonPerbankan*. Penerbit PPM.

The digital economy: rethinking promise and peril in the age of networked intelligence. (2015). *Choice Reviews Online*. https://doi.org/10.5860/choice.189656

Toma, S.-V., Alexa, I. V., & Şarpe, D. A. (2014). Identifying the Risk in Higher Education Institutions. *Procedia Economics and Finance*, *15*(14), 342–349. https://doi.org/10.1016/s2212-5671(14)00520-6