MANAJEMEN RISIKO TEKNOLOGI INFORMASI: STUDI KASUS PADA PERUSAHAAN JASA

Achmad Reza Viyanto; Okhran Steve Latuihamallo; Franky Mangihut Tua; Anderes Gui; Suryanto

Computerized Accounting Department, School of Information Systems, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
anderesgui@binus.edu

ABSTRACT

The purpose of this study is to identify and quantify risks that may occur any time in the application of information technology in a company, as well as to provide information on the risks associated with the security of information technology system of the company. The methods used are: data collection and analysis techniques. Data collection includes: literature and field studies, in which the field study is conducted by interview and observation. Analytical technique used in the measurement of risk is OCTAVE-S. The results found the risks associated with security management, contingency planning, vulnerability management, as well as design and security architecture. It iscocluded from this this study that there are still a lot of risks that can threaten companies such as lack of contingency and disaster recovery plan.

Keywords: *risk measurement, information technology, security, vulnerability*

ABSTRAK

Tujuan dari penelitian ini adalah mengidentifikasi dan mengukur risiko-risiko yang sewaktu-waktu dapat terjadi dalam penerapan teknologi informasi pada perusahaan, serta memberikan informasi mengenai risiko-risiko yang berkaitan dengan keamanan sistem teknologi informasi pada perusahaan. Metode yang digunakan yaitu: teknik pengumpulan data dan teknik analisis. Teknik pengumpulan data terdiri dari: studi pustaka, dan studi lapangan, di mana studi lapangan dilakukan dengan wawancara dan pengamatan. Teknik analisis yang digunakan dalam pengukuran risiko adalah OCTAVE-S. Hasil yang dicapai yaitu ditemukannya risiko-risiko yang berkaitan dengan manajemen keamanan, rencana contigency, manajemen kerentanan, serta desain dan arsitektur keamanan. Simpulan dari penelitian ini adalah masih terdapat berbagai risiko yang dapat mengancam perusahaan seperti tidak adanya rencana contigency dan disaster recovery plan.

Kata kunci: *pengukuran risiko, teknologi informasi, keamanan, kerentanan*

PENDAHULUAN

Penggunaan teknologi informasi di dalam perusahaan merupakan suatu elemen penting untuk menunjang efektifitas dan efisiensi proses bisnis perusahaan. Teknologi informasi ini diharapkan oleh perusahaan dapat meningkatkan mutu pelayanan sehingga tercapainya tujuan bisnis perusahaan. Pemanfaatan teknologi informasi harus diiringi dengan pengelolaan yang tepat dan relevan sehingga dapat meminimalisasi risiko-risiko yang mungkin timbul di dalam proses bisnis.

Menurut Peltier (2001, p224) "*Risk management is the process of identifying risks, risk-mitigating measures, the budgetary effect of implementing decisions related to the acceptance, avoidance, or transfer of risk.*"

Menurut Alberts dan Dorofee (2003, p298) "*risk management is the ongoing process of identifying risks and implementing plans to address them*."

Menurut Turban, Rainer, dan Potter (2009, p6), *"Information technology relates to any computer-based to that people use to work with information and to support the information and information processing needs of an organization."*

Menurut Trieschmann, Hoyt, Sommer (2005, p11), *"Risk management is the process used to systematically manage risk exposures"*.

Jadi, manajemen risiko adalah suatu proses identifikasi, mengatur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain: mentransfer risiko pada pihak lain, menghindari risiko, mengurangi efek buruk dari risiko, dan menerima sebagian maupun seluruh konsekuensi dari risiko tertentu.

Menurut Purtell (2007), usaha untuk meminimalisasi risiko-risiko yang mungkin terjadi ataupun untuk mengatasi risiko-risiko yang telah terjadi di dalam proses bisnis dapat dilakukan dengan manajemen risiko. Manajemen risiko memiliki peranan yang sangat penting untuk pengambilan keputusan terhadap risiko-risiko yang terjadi, membantu pengaturan risiko teknologi informasi, membantu perkembangan proses bisnis dan memberikan keuntungan, efisiensi terhadap pengendalian risiko, melakukan penghapusan nilai-nilai sisa, pengurangan terhadap beban, dan manajemen sumber daya yang efektif.

Selain itu, menurut riset pada tahun 2004 yang telah dilakukan oleh Brown (2006), perusahaan yang memiliki spesialis IT dalam pengambilan keputusan untuk pengembangan arsitektur dan infrastruktur adalah perusahaan yang memiliki efektifitas paling baik di antara 256 perusahaan yang telah disurvei.

Menurut Pathak (2005), semua sistem keamanan memiliki kelemahan. Ketika teknologi dikaitkan dengan keamanan sistem, kelemahan sistem tersebut menjadi lebih rumit dan sulit untuk ditemukan dan dilindungi. Untuk membentuk sebuah sistem keamanan yang baik, perusahaan harus melakukan pengujian terhadap sejumlah ancaman untuk menemukan kerentanan-kerentanan yang baru.

Pengelolaan informasi di dalam perusahaan tidak terlepas dari adanya kepercayaan antara pihak manajemen dengan karyawan. Menurut Veiga dan Eloff (2007) kepercayaan adalah elemen yang penting dalam membangun keamanan informasi di dalam lingkungan teknologi informasi. Jika manajemen percaya kepada karyawan, dan begitu pula sebaliknya maka akan memudahkan untuk

mengimplementasikan prosedur yang baru dan mengarahkan karyawan untuk melewati perubahan prilaku terhadap keamanan informasi.

Morse, sebuah perusahaan IT asal Inggris, telah melakukan survei pada 1.460 karyawan perusahaan tersebut. Ternyata, lebih dari setengahnya (57%) di antara mereka menggunakan waktu kerja selama 40 menit per minggu, atau kira-kira satu minggu dalam setahun hanya untuk mengakses situs jejaring sosial, seperti Facebook dan Twitter. Kegiatan mengakses situs jejaring sosial ini dapat merugikan sejumlah pengusaha. Terutama bagi perusahaan yang karyawannya berinteraksi di sana selama jam kerja dan menurunkan produktivitas. Bila dikalkulasikan, diperkirakan bahwa pebisnis di seluruh Inggris mengalami kerugian total sekitar 1,38 miliar poundsterling atau 21 triliun rupiah per tahun akibat waktu yang disalahgunakan oleh karyawannya.

Contoh kasus di atas memberikan suatu gambaran mengenai kerugian yang diakibatkan oleh lemahnya sistem pengendalian dalam mengelola penggunaan teknologi informasi. Teknologi informasi yang sebelumnya diharapkan oleh perusahaan untuk meningkatkan produktivitas karyawan justru membawa dampak yang merugikan karena kurangnya pemahaman mengenai dimensi risiko teknologi informasi. Kemudian pemahaman itu juga seharusnya diikuti dengan pengetahuan tentang cara terbaik dalam mengatasinya, tidak hanya dengan melakukan pengukuran terhadap risiko, tetapi dengan mendefinisikan penanggulangan apabila risiko-risiko tersebut terjadi dan tentu saja mengimplementasikan manajemen risiko. Oleh karena itu perlu dilakukan pengukuran risiko teknologi informasi.

METODE

Untuk mengumpulkan data-data yang dibutuhkan pada penelitian ini, dilakukan wawancara dengan pihak HRD dan pihak TI dengan upaya untuk mengetahui risiko-risiko apa saja yang terjadi atau kemungkinan terjadi pada perusahaan. Metode OCTAVE-S tersebut terdiri dari tiga tahap (Alberts, et al., 2003,), yaitu: (1) membangun aset berbasis profil ancaman; (2) mengidentifikasi kerentanan infrastruktur; dan (3) mengembangkan strategi keamanan dan perencanaan.

Dari ketiga tahap tersebut di dalamnya terdapat 5 proses yang terdiri dari 16 aktivitas dan 30 langkah. Lima proses tersebut yaitu: (1) mengidentifikasi informasi organisasi, yang terdiri dari 3 aktivitas dan 4 langkah; (2) membuat profil ancaman, yang terdiri dari 3 aktivitas dan 12 langkah; (3) memeriksa perhitungan infrastruktur yang berhubungan dengan aset kritis, yang terdiri dari 2 aktivitas dan 5 langkah; (4) identifikasi dan analisis risiko, yang terdiri dari 3 aktivitas dan 3 langkah; (5) mengembangkan strategi perlindungan dan rencana mitigasi, yang terdiri dari 5 aktivitas dan 6 langkah.

Di dalam metode OCTAVE-S terdapat beberapa kategori risiko yang merupakan dasar pengukuran risiko OCTAVE-S, di mana kategori risiko ini menjadi tolak ukur wajib dalam melakukan penelitian. Kategori tersebut yaitu: Kesadaran Keamanan dan Pelatihan; Strategi Keamanan; Manajemen Keamanan; Peraturan dan Kebijakan Keamanan; Kolaborasi Manajemen Keamanan; Rencana Kemungkinan; Pengendalian Akses Fisik; Pemantauan dan Audit Keamanan Fisik; Manajemen jaringan dan sistem; Pemantauan dan Audit Keamanan TI; Pengesahan dan Otorisasi; Manajemen Kerentanan; Enkripsi; Desain dan Arsitektur Keamanan; Manajemen Insiden.

Menurut Alberts, et al. (2003), selama mengevaluasi OCTAVE-S, tim analisis melibat keamanan dari beberapa perspektif, memastikan bahwa rekomendasi yang dicapai sesuai dengan keseimbangan berdasarkan kebutuhan organisasi.

Hasil utama dari OCTAVE-S, yaitu: Strategi perlindungan organisasi yang luas, Rencana mitigasi risiko, Daftar tindakan. Hasil OCTAVE-S yang berguna lainnya, yaitu: Daftar informasi penting terkait dengan aset yang mendukung tujuan bisnis dan sasaran organisasi, hasil survei menunjukkan sejauh mana organisasi mengikuti praktek keamanan yang baik, profil risiko untuk setiap aset kritis menggambarkan jarak antara risiko terhadap aset.

HASIL DAN PEMBAHASAN

Analisis Praktik Keamanan

Hasil analisis praktik keamanan pada perusahaan, yaitu:

Kesadaran Keamanan dan Pelatihan

Saat ini kesadaran keamanan dan pelatihan telah dijalankan dengan cukup baik, dikarenakan para karyawan memahami peran keamanan dan tanggung jawab mereka dalam mengikuti kebijakan perusahaan, meskipun pelatihan karyawan mengenai keamanan tidak dilakukan dengan rutin.

Strategi Keamanan

Strategi bisnis yang dimiliki oleh perusahaan selalu mempertimbangkan segi keamanan, segi tujuan dan sasaran perusahaan. Strategi keamanan, tujuan dan sasaran perusahaan tersebut telah didokumentasikan dan dikaji serta diperbaharui sekaligus dikomunikasikan. Namun, hal tersebut tidak dilakukan secara rutin karena pembahasan mengenai strategi keamanan akan dibahas secara detail pada saat periodik tertentu saja.

Manajemen Keamanan

Perusahaan telah melakukan pengalokasian dan sumber daya yang cukup untuk aktivitas keamanan informasi. Peran keamanan dan tanggung jawab sudah dijelaskan kepada semua karyawan. Sebagian karyawan telah melaksanakan dengan baik tugas dan tanggung jawab yang berkaitan dengan keamanan informasi dan memberikan sanksi kepada karyawan yang terlibat dalam permasalahan keamanan informasi.

Peraturan dan Kebijakan Keamanan

Peraturan dan kebijakan perusahaan selalu ditinjau dan diperbaharui secara berkala, dan dikaji secara menyeluruh, namun tidak didokumentasikan.

Kolaborasi Manajemen Keamanan

Perusahaan telah memiliki kebijakan dan prosedur dalam bekerja sama dengan perusahaan lain, seperti: melindungi informasi milik perusahaan lain, memahami kebijakan keamanan dan prosedur perusahaan lain serta membatasi akses bagi pihak yang tidak berkepentingan.

Rencana Kemungkinan

Saat ini perusahaan belum melakukan analisis terhadap hal-hal yang berkaitan dengan kegiatan operasional, aplikasi-aplikasi dan data penting yang ada di perusahaan. Selain itu perusahaan

belum memiliki dokumentasi atas peninjauan dan pengujian terhadap kontinuitas bisnis atau rencana operasi darurat untuk menanggulangi keadaan darurat.

Pengendalian Akses Fisik

Perusahaan telah memiliki pengendalian yang baik terhadap akses fisik, seperti adanya prosedur dan rencana fasilitas keamanan dalam menjaga lokasi, bangunan, namun belum didokumentasikan dan diuji. Perusahaan telah memiliki prosedur terutama dalam mengelola pengunjung dan pengendalian akses fisik ke tempat kerja, perangkat keras, dan perangkat lunak. Area kerja yang banyak menggunakan komputer dan komponen lainnya yang memungkinkan akses ke informasi yang sensitif dan secara fisik menjamin untuk mencegah akses yang tidak sah.

Pemantauan dan Audit Keamanan Fisik

Saat ini perusahaan telah memiliki catatan pemeliharaan yang disimpan kedalam dokumen perbaikan dan modifikasi dari komponen fasilitas fisik. Tindakan individu atau kelompok yang berkaitan dengan semua media yang dikontrol secara fisik, dapat dipertanggungjawabkan. Pemeriksaan dan pemantauan dilakukan secara rutin, memeriksa catatan dan melihat kejanggalan-kejanggalan yang ada, dan mengambil tindakan korektif (perbaikan) jika diperlukan.

Manajemen jaringan dan sistem

Perusahaan telah mengelola sistem dan jaringan dengan baik, hal tersebut dapat dilihat dari adanya penggunaan sistem wireless di dalam jaringan LAN. Perusahaan telah melindungi informasi sensitif di tempat yang aman. Dan pihak yang tidak mempunyai wewenang yang berkaitan dengan informasi tersebut tidak dapat mengaksesnya.

Pemantauan dan Audit Keamanan TI

Perusahaan telah melakukan pemantauan dan mengaudit sistem dan jaringan perusahaan secara baik. Perusahaan mengaktifkan firewall yang berfungsi sebagai sistem keamanan yang melindungi sistem komputer yang berjalan.

Pengesahan dan Otorisasi

Perusahaan telah melakukan pengontrolan yang baik sesuai dengan akses yang tepat dan pengesahan yang konsisten di dalam hal perizinan file dan konfigurasi jaringan. Perusahaan juga telah melakukan pembatasan akses terhadap informasi ataupun sistem sensitif.

Perusahaan memiliki dokumentasi kebijakan dan prosedur yang mengatur hak akses secara individu maupun kelompok. Hal ini akan mengatur jaminan keamanan terhadap informasi yang bersifat sensitif. Informasi tidak dapat diakses ataupun diubah ke dalam bentuk apapun oleh pihak yang tidak memiliki wewenang.

Manajemen Kerentanan

Perusahaan belum memiliki manajemen kerentanan dengan baik karena perusahan tidak meninjau atau menilai sumber informasi mengenai kerentanan informasi, peringatan dan keamanan informasi dan pemberitahuan. Hal lainnya adalah perusahaan tidak mengidentifikasi komponen infrastruktur untuk dievaluasi serta tidak memberikan penafsiran dan menanggapi hasilnya.

Enkripsi

Perusahaan telah melakukan pengendalian keamanan yang sesuai dengan kebutuhan perusahaan untuk melindungi informasi yang sensitif, selama dalam penyimpanan dan transmisi data. Protokol enkripsi juga digunakan ketika mengelola sistem, *router*, dan *firewall*.

Desain dan Arsitektur Keamanan

Perusahaan sudah mempunyai sistem desain dan arsitektur keamanan yang baik terhadap sistem yang akan digunakan di perusahaan dan sistem tersebut akan direvisi dengan mempertimbangan hal-hal seperti: strategi keamanan, kebijakan dan prosedur. Namun, perusahaan belum mempunyai aplikasi yang up-to-date untuk menunjukkan arsitektur keamanan dari perusahaan dan topologi jaringan.

Manajemen Insiden

Dalam mengelola insiden di dalam perusahaan, perusahaan memiliki prosedur yang didokumentasikan untuk mengidentifikasi, melaporkan dan menanggapi dugaan pelanggaran keamanan dan insiden. Namun dalam penanganannya, perusahaan belum melakukan verifikasi dan diperbaharui secara periodik.

Profil Ancaman

Adapun aset-aset kritis yang terdapat di perusahaan, yaitu: (a) Aplikasi *Group health insurance*, (b) Database Server, (c) Jaringan, dan (d) PC.

Kebutuhan Keamanan pada Aset Kritis

Kebutuhan keamanan terhadap seluruh aset-aset penting yang ada di perusahaan terdiri dari tiga hal, yaitu: kerahasiaan informasi, integritas data, dan adanya ketersediaaan data dan informasi saat dibutuhkan. Kebutuhan keamanan yang paling penting dalam perusahaan terletak pada ketersediaan data atau informasi, karena jika data atau informasi yang dibutuhkan tidak tersedia maka aktivitas proses bisnis perusahaan tidak dapat berjalan dengan lancar.

Ancaman pada Aset Kritis

Ancaman pada aset kritis perusahaan dapat terjadi melalui dua akses, yaitu: akses fisik maupun akses jaringan, dan setiap akses mempunyai dua aktor, yaitu: aktor yang berasal dari dalam perusahaan dan aktor yang berasal dari luar perusahaan. Motif pelaku dalam melakukan ancaman dibagi menjadi dua, yaitu: ancaman yang dilakukan dengan sengaja dan ancaman yang dilakukan dengan tidak sengaja. Dari motif pelaku tersebut, mengakibatkan kemungkinan terjadinya penyingkapan, modifikasi, penghancuran dan gangguan.

Infrastruktur yang berhubungan dengan Aset Kritis

Sistem dan komponen yang berkaitan dengan aset kritikal perusahaan (*group health insurance*) yaitu: PC, jaringan, dan database server. PC, sangat berkaitan dalam penggunaan *group health insurance* untuk menginput data klien serta memilih bentuk proteksi yang akan digunakan. Database server (MS SQL Server) juga digunakan oleh perusahaan untuk menunjang penggunaan aplikasi *group health insurance*.

Hasil Evaluasi Dampak Ancaman

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses jaringan yang dilakukan oleh pihak dalam perusahaan secara tidak sengaja, yaitu: (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi dan bernilai tinggi untuk penghancuran dan gangguan dan (2) dampak terhadap keamanan bernilai rendah untuk modifikasi dan gangguan serta bernilai sedang untuk penghancuran.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses jaringan yang dilakukan oleh pihak dalam perusahaan secara sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi serta bernilai tinggi untuk penghancuran dan gangguan; (2) dampak terhadap keamanan bernilai sedang untuk gangguan serta bernilai rendah untuk modifikasi dan penghancuran.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses jaringan yang dilakukan oleh pihak luar perusahaan secara tidak sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi serta bernilai tinggi untuk penghancuran dan gangguan; (2) dampak terhadap keamanan bernilai rendah untuk modifikasi dan gangguan sedangkan bernilai sedang untuk penghancuran.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance* melalui akses jaringan yang dilakukan oleh pihak luar perusahaan secara sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi serta bernilai tinggi untuk penghancuran dan gangguan; (2) dampak terhadap keamanan bernilai sedang untuk gangguan sedangkan bernilai rendah untuk modifikasi dan penghancuran.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses fisik yang dilakukan oleh pihak dalam perusahaan secara tidak sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi dan bernilai tinggi untuk penghancuran serta bernilai rendah untuk gangguan; (2) dampak terhadap keamanan bernilai sedang untuk modifikasi dan bernilai rendah untuk penghancuran dan gangguan.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses fisik yang dilakukan oleh pihak dalam perusahaan secara sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi serta bernilai tinggi terhadap gangguan dan penghancuran; (2) dampak terhadap keamanan bernilai sedang untuk gangguan serta bernilai rendah untuk modifikasi dan penghancuran.

Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses fisik yang dilakukan oleh pihak luar perusahaan secara tidak sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi dan gangguan serta bernilai tinggi untuk penghancuran; (2) dampak terhadap keamanan bernilai rendah untuk modifikasi serta bernilai sedang untuk penghancuran dan gangguan. Dampak ancaman pada aset kritikal (aplikasi *group health insurance*) melalui akses fisik yang dilakukan oleh pihak luar perusahaan secara sengaja, yaitu (1) dampak terhadap produktivitas bernilai sedang untuk modifikasi dan bernilai tinggi untuk penghancuran dan gangguan; (2) dampak terhadap keamanan bernilai sedang untuk gangguan serta bernilai rendah untuk modifikasi dan penghancuran.

Kriteria Kemungkinan

Frekuensi terjadinya ancaman pada perusahaan masih tergolong rendah karena ancaman yang terjadi masih di bawah tiga kali dalam setahun. Saat ini, ancaman-ancaman yang terjadi pada

perusahaan masih dapat diatasi oleh pihak dalam perusahaan. Pengukuran ini berlaku untuk semua ancaman pada aset penting, baik yang disengaja maupun yang tidak sengaja.

Peluang dari Ancaman

Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan, yaitu:
Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong rendah dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan, yaitu:
Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan, yaitu:
Besarnya motif pihak luar perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak luar perusahaan yang secara tidak sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan, yaitu:
Besarnya motif pihak luar perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak luar perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak luar perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik, yaitu:
Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong rendah dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik, yaitu:
Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik, yaitu: Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik, yaitu: Besarnya motif pihak luar perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak luar perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang. dan besarnya motif pihak luar perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Strategi Perlindungan

Dari penelitian yang dilakukan pada Perusahaan dengan menggunakan pendekatan OCTAVE-S, ditemukan beberapa risiko dari penerapan teknologi informasi yang berkaitan dengan praktik keamanan yang ada pada perusahaan. Risiko-risiko yang ditemukan berfokus pada manajemen keamanan, rencana kemungkinan, manajemen kerentanan, serta desain dan arsitektur keamanan. Strategi perlindungan yang akan direncanakan dalam perusahaan, yaitu: manajemen keamanan, rencana kemungkinan, manajemen kerentanan, dan desain dan arsitektur keamanan.

Manajemen Keamanan

Saat ini perusahaan belum melakukan penilaian risiko terhadap keamanan informasi. Jika terjadi risiko maka divisi IT yang akan langsung mengambil langkah-langkah dalam meminimalisir risiko keamanan informasi tersebut. Selain itu perusahaan juga tidak memiliki kebijakan dan prosedur mengenai penghentian kerja terhadap pihak karyawan yang terlibat dalam permasalahan keamanan informasi

Rencana Kemungkinan

Saat ini perusahaan belum melakukan operasi analisis terhadap operasi, aset-aset dan data penting yang dianggap dapat memberikan kontinuitas bisnis pada saat bencana telah terjadi. Perusahaan ini pun belum memiliki rencana pemulihan bencana dan mempertimbangkan rencana fisik untuk keberlangsungan bisnis.

Manajemen Kerentanan

Perusahaan belum meninjau atau menilai sumber informasi mengenai kerentanan informasi, peringatan akan keamanan informasi dan pemberitahuan. Selain itu perusahaan juga tidak melakukan identifikasi terhadap komponen infrastruktur untuk di evaluasi secara periodik. Dan prosedur manajemen kerentanan belum dimonitori dan ditinjau serta di-update secara berkala.

Desain dan Arsitektur Keamanan

Perusahaan belum memiliki hasil penilaian risiko keamanan yang dijadikan pertimbangan sebagai pertimbangan dalam membentuk sistem arsitektur dan desain baru maupun sistem yang direvisi. Perusahaan juga belum memilik aplikasi yang up-to-date yang menunjukkan arsitektur keamanan dari perusahaan dan topologi jaringan.

Pendekatan Mitigasi

Berdasarkan kertas kerja profil risiko yang terdapat pada langkah OCTAVE-S, ada pendekatan mitigasi yang dilakukan oleh perusahaan atas ancaman yang terjadi di perusahaan, baik ancaman yang bermotif sengaja maupun yang tidak disengaja pada pihak internal perusahaan dan pihak eksternal perusahaan melalui akses jaringan dan akses fisik.

Perusahaan akan mengambil tindakan mitigasi risiko pada praktik keamanan melalui akses jaringan yang dilakukan oleh pihak dalam perusahaan. Kegiatan mitigasi berfokus pada satu aktivitas praktik keamanan, yaitu: (1) manajemen keamanan dan (2) arsitektur dan desain keamanan. Sedangkan untuk pihak luar, perusahaan belum melakukan mitigasi. dan tindakan mitigasi risiko pada akses fisik yang diakibatkan oleh pihak dalam dan pihak luar perusahaan berfokus pada (3) rencana kemungkinan dan (4) manajemen kerentanan rencana mitigasi risiko.

Rencana Mitigasi Risiko

Rencana mitigasi risiko yang berkaitan dengan manajemen keamanan untuk praktik keamanan, meliputi: (1) dibentuknya suatu tim manajemen risiko untuk melakukan penilaian risiko, sehingga dapat meminimalisir risiko sejak awal; (2) mendokumentasikan mengenai tugas dan tanggung jawab keamanan informasi untuk semua karyawan dalam perusahaan; (3) melaksanakan program pelatihan kesadaran keamanan perusahaan yang mencakup informasi tentang proses manajemen keamanan perusahaan. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu.

Rencana mitigasi risiko yang berkaitan dengan rencana kemungkinan, meliputi: (1) melakukan analisis terhadap operasional, aplikasi-aplikasi, dan data penting yang dianggap dapat memberikan kontinuitas bisnis untuk penanggulangan bencana; (2) mendokumentasikan pengujian dan peninjauan terhadap kontinuitas bisnis, rencana pemulihan bencana, dan kemungkinan rencana untuk menanggulangi keadaan darurat.

Rencana mitigasi risiko yang berkaitan dengan manajemen kerentanan, meliputi: (1) mendokumentasikan prosedur yang digunakan untuk mengelola kerentanan, seperti: memilih alat evaluasi kerentanan, menjaga serangan dan pengetahuan tentang kerentanan secara up-to-date, serta menilai sumber informasi yang berkaitan dengan kerentanan informasi; (2) mengidentifikasikan komponen infrastruktur untuk dievaluasi; (3) mengelola tempat penyimpanan yang paling aman dan menjaga kerentanan data; (3) penilaian kerentanan teknologi dilakukan secara periodik.

Rencana mitigasi risiko yang berkaitan dengan desain dan arsitektur keamanan, meliputi: memiliki hasil penilaian risiko keamanan yang akan menjadi pertimbangan terhadap pembangunan sistem arsitektur dan desain baru, maupun sistem yang direvisi.

Perubahan Strategi Perlindungan

Perubahan strategi perlindungan yang berkaitan dengan manajemen keamanan untuk praktik keamanan, meliputi: (1) melakukan penilaian risiko dilakukan secara rutin; (2) mengadakan pelatihan mengenai kesadaran keamanan perusahaan yang mencakup informasi tentang proses manajemen keamanan perusahaan. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu; (3) mendokumentasikan tugas dan tanggung jawab keamanan informasi untuk semua karyawan dalam perusahaan.

Perubahan strategi perlindungan yang berkaitan dengan rencana *contigency*, meliputi: (1) melakukan analisis terhadap operasional, aplikasi-aplikasi dan data penting yang dianggap dapat

memberikan kontinuitas bisnis untuk penanggulangan bencana; (2) memiliki rencana pemulihan bencana yang ditinjau, diuji dan didokumentasikan.

Perubahan strategi perlindungan yang berkaitan dengan manajemen kerentanan, meliputi: (1) mengidentifikasikan komponen infrastruktur untuk dievaluasi; (2) melakukan penilaian kerentanan teknologi yang dilakukan secara periodik; (3) memiliki prosedur manajemen kerentanan data yang didokumentasikan.

Perubahan strategi perlindungan yang berkaitan dengan desain dan arsitektur kemananan, meliputi: memiliki hasil penilaian risiko keamanan yang akan menjadi pertimbangan terhadap pembangunan sistem arsitektur dan desain baru, maupun sistem yang direvisi.

Identifikasi Langkah Selanjutnya

Dalam mendukung pelaksanaan hasil pengukuran risiko teknologi informasi OCTAVE-S, ada beberapa hal yang menjadi pertimbangan perusahaan, di mana manajemen perusahaan harus membuat suatu strategi bisnis sebagai prioritas bagi keamanan perusahaan dan melakukan evaluasi secara berkala agar dapat disusun rencana stategi untuk penangulangan risiko. Serta perusahaan dapat mempertimbangan apakah metode OCTAVE-S merupakan metode terbaik dalam melakukan pengukuran risiko guna menjaga aset-aset perusahaan.

PENUTUP

Dari hasil analisis yang dilakukan, diperoleh beberapa simpulan, yaitu: (1) perusahaan belum menerapkan manajemen *risiko* TI secara menyeluruh. Hal ini dapat dilihat dengan tidak adanya rencana *contigency* dan *disaster recovery plan*; (2) tidak memiliki alokasi dana untuk melakukan pelatihan kesadaran dan keamanan secara berkala; (3) perusahaan telah mengelola sistem keamanan dan jaringan dengan baik, dapat dilihat dari adanya akses terbatas terhadap informasi yang bersifat sensitif.

DAFTAR PUSTAKA

Alberts, C dan Dorofee, A. (2003). *Managing information security risks*. Canada: Adisson Wesley.

Alberts, C., Dorofee, A., Stevens, J., & Woody C. (2003). *OCTAVE-S Implementation Guide, Version 1.0*. Pittsburgh: Carnegie Mellon University.

Brown, W. C. (2006). *IT Governance, Architectural Competency, and the Vasa. Information Management & Computer Security, 14*. Diakses 25 Febuariuari 2010 dari http://proquest.umi.com/pqdweb?did=1073465011&sid=5&Fmt=3&clientId=68814&RQT=309&VName=PQD
http://proquest.umi.com/pqdweb?did=1368985541&sid=4&Fmt=4&clientId=68814&RQT=309&VName=PQD

Pathak, J. (2005). *Risk Management, Internal Controls, and Organizational Vulnerabilities. Managerial Auditing Journal, 20*. Diakses 25 Febuari 2010 dari http://proquest.umi.com/pqdweb?did=907062421&sid=3&Fmt=3&clientId=68814&RQT=309&VName=PQD

Peltier, T.R. (2001). *Information Security Risk Analysis.* Auerbach, United Stated.

Purtell, T. (2007). A New View on IT Risk. *Risk Management, 54*. Diakses 25 Febuari 2010 dari

Rainer, R. K., Turban, E., & Potter, E. (2009). *Introduction to Information Systems: Supporting and Transforming Business (International Student Version)*. New York: John Wiley & Sons.

Trieschmann, J. S., Hoyt, R. E., & Sommer, D. W. (2005). *Risk Management and Insurance,* 12th edition. Mason: Thomson South-Western.

Veiga, A. D. & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management, 24.* Diakses 25 Febuari 2010 dari http://proquest.umi.com/pqdweb?did=1395622361&Fmt=3&clientId=68814&RQT=309&VName=PQD