PENGUKURAN RESIKO TEKNOLOGI INFORMASI (TI) DENGAN METODE OCTAVE-S

Anderes Gui[1], Sanyoto Gondodiyoto[2], Irvan Timotius[3]

[1, 2, 3]Jurusan Komputerisasi Akuntansi, Fakultas Ilmu Komputer, Universitas Bina Nusantara, Jln. K.H. Syahdan No.9, Palmerah, Jakarta Barat 11480
anderesgui@binus.edu

ABSTRACT

Article presented a measurement of Information Technology (IT) risk levels and identify security practices which were suitable in the risk overcoming, as noted in PTNL. Company was also expected to be more alert to the risk impacts of information technology which might occur in PTNL. Analytical method used was OCTAVE-S method. This method was used in a risk measurement of information technology risk, with some steps which had important roles in searching for the measurement results effectively and efficiently, which were applied in PTNL. The results which will be achieved were to give overall results of risk measurement occurred at the company, either the plus or minus, and provide recommendations which are expected to solve and correct the minus or problems which occurred in PTNL. Conclusion states that the risk measurement of information technology performed in PTNI has successfully minimized the risks that can threaten the company's security.

Keywords: *measurement, risk, Information Technology (IT), OCTAVE-S method*

ABSTRAK

Artikel menjelaskan pengukuran tingkat risiko Teknologi Informasi (TI) dan identifikasi praktik keamanan yang cocok dalam penanggulangan risiko, di PTNL. Diharapkan juga perusahaan dapat lebih waspada terhadap dampak risiko TI yang mungkin terjadi dalam PTNL. Metode analisis yang digunakan adalah metode OCTAVE-S. Metode ini digunakan dalam pengukuran risiko TI, dengan beberapa langkah yang berperan penting dalam mencari hasil pengukuran secara efektif dan efisien, yang diterapkan pada PTNL. Hasil yang ingin dicapai adalah memberikan keseluruhan hasil pengukuran risiko yang terjadi pada perusahaan, baik kelebihannya maupun kekurangannya, serta memberikan rekomendasi-rekomendasi yang diharapkan dapat mengatasi dan memperbaiki kekurangan maupun permasalahan yang terjadi dalam PTNL. Disimpulkan pengukuran risiko TI yang dilakukan pada PTNL telah berhasil meminimalisasi risiko-risiko yang dapat mengancam keamanan perusahaan.

Kata kunci: *pengukuran, risiko, Teknologi Informasi, metode OCTAVE-S*

PENDAHULUAN

Berkembangnya TI yang sangat pesat saat ini, telah menuntut setiap perusahaan untuk terus bergerak mengikutinya. Oleh karena itu, untuk dapat menghadapi ketatnya persaingan, perusahaan dituntut untuk selalu berkembang, dengan melakukan pengambilan keputusan secara cepat, tepat, dan efisien.

TI pada perusahaan, selain memberikan keuntungan juga membawa risiko yang beragam seperti timbulnya kesalahan tanpa disengaja. Misalnya adalah kehilangan data akibat *server* yang terserang virus dan kesalahan yang terjadi karena faktor kesengajaan atau kecurangan. Risiko-risiko yang timbul tersebut akan menimbulkan dampak kerugian bagi perusahaan, baik secara finansial ataupun non finansial.

Oleh karena itu, diperlukan suatu pengukuran terhadap risiko yang ada dalam penerapan TI. Pengukuran risiko TI berguna untuk mengetahui profil risiko TI, analisis terhadap risiko, dan juga melakukan respon terhadap risiko, sehingga tidak terjadi dampak-dampak yang kemungkinan muncul dari risiko tersebut. Penerapan TI didukung dengan sistem pengamanan yang kuat, prosedur yang baik, otorisasi yang baik, dan pemeliharaan berkala terhadap sumber daya komputer, sehingga dapat menjamin keamanan aset perusahaan, pemeliharaan integritas data, dan penggunaan sumber daya yang tepat.

Metode Penelitian

Pendekatan yang dipakai untuk melakukan risiko TI bersifat kualitatif. Metode yang dipakai berupa studi kasus pada PTNL. Teknik yang melengkapi metode penelitian tersebut antara lain metode pengumpulan data dan metode analisis.

Metode Pengumpulan Data

Pengumpulan data dilakukan antara lain dengan mencari ke berbagai sumber terpercaya sebagai berikut. Pertama adalah metode pustaka, yaitu mengumpulkan data dengan menggunakan sumber berupa buku atau bahan dari perpustakaan sebagai panduan dalam penyusunan paper ini. Perpustakaan tempat penulis melakukan riset berlokasi di Perpustakaan Universitas Bina Nusantara, Kampus Anggrek lantai 1. Buku–buku yang digunakan adalah buku yang memuat pengertian TI, risiko TI, manajemen TI dan manajemen risiko TI, serta yang diutamakan adalah buku yang memuat metode OCTAVE-S sebagai dasar materi pengukuran risiko TI di

perusahaan. Kedua adalah metode lapangan, yaitu dengan meninjau langsung ke PTNL, yang berlokasi di Jln. Raya Serang KM 8 (Jln. Telesonik), Tangerang, dengan tujuan untuk memperoleh data yang dibutuhkan dalam penelitian.

Adapun cara yang digunakan adalah: wawancara (*interview*). Proses memperoleh data dengan cara tanya jawab secara langsung melalui pihak yang berkepentingan dalam perusahaan, sehingga didapatkan data yang berkualitas; berikutnya adalah observasi. Dengan melakukan pengamatan dan peninjauan secara langsung terhadap objek yang akan diteliti, penulis disini berkaitan dengan kondisi TI yang dipakai perusahaan, yang mencakup *hardware*, *software*, jaringan, dan aplikasi yang diterapkan dalam perusahaan; yang terakhir adalah kuisioner. Proses pengumpulan sejumlah data secara acak, yang dibagikan kepada beberapa responden mengenai sistem pada perusahaan. Data yang sudah terkumpul akan digunakan dalam melakukan pengukuran risiko pada PTNL.

Metode Analisis

Dari berbagai macam teknik yang ada untuk mengukur risiko TI, maka penulis memutuskan untuk memakai OCTAVE-S. Metode ini merupakan variasi dari pendekatan OCTAVE, yang dikembangkan untuk mengukur risiko TI bagi organisasi yang beranggotakan 20 sampai 80 orang, dan diharapkan juga mempunyai 3 sampai 5 orang yang memahami tentang keamanan.

Landasan Teori

Alberts, Dorofee, Stevens, dan Woody (2001: 43), "*Risk is the Possibility of Suffering Harm or Loss"* (risiko adalah kemungkinan untuk menderita kerugian atau kehilangan). Menurut Hughes (2006: 36), kategori risiko TI antara kehilangan informasi potensial dan pemulihannya adalah sebagai berikut. Pertama adalah keamanan. Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berotoritas. Ini termasuk kejahatan komputer, kebocoran internal, dan terorisme *cyber*. Kedua adalah ketersediaan. Risiko yang datanya tidak dapat diakses seperti setelah kegagalan sistem, karena kesalahan manusia, perubahan konfigurasi, kurangnya pengurangan arsitektur atau akibat lainnya. Ketiga adalah daya pulih. Risiko di mana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah sebuah kejadian keamanan atau ketersediaan seperti kegagalan perangkat lunak atau keras, ancaman eksternal, atau bencana alam. Keempat adalah performa. Risiko di mana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi, dan topografi informasi teknologi yang beragam. Kelima adalah daya skala. Risiko yang perkembangan bisnis, pengaturan *bottleneck,* dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif. Keenam adalah ketaatan. Risiko yang manajemen atau penggunaan informasinya melanggar keperluan *regulator*. Yang dipersalahkan dalam hal ini mencakup regulasi pemerintah, panduan pengaturan korporat, dan kebijakan internal.

Selain itu, menurut Noshworthy (2000: 600), "*risk management is implementation of measures aimed at reducing the likelihood of those threats occurring and minimizing any damages if they do. Risk analysis and risk control form the basis of risk management where risk control is the application of suitable controls to gain a balance between security and usability"*.

Proses Bisnis

Setiap pelanggan akan dikenakan *minimum order*, biaya minimum yang harus dikeluarkan dalam melakukan pemesanan senilai Rp 400.000,00. Apabila pemesanan tidak mencapai nominal yang diinginkan, maka perusahaan tidak akan menerima pesanan pelanggan. Pembayaran dapat dilakukan dengan mentransfer ke nomor rekening perusahaan maupun *cash*. Pembayaran *cash* akan langsung diterima *sales*. Dari *sales* pembayaran tersebut akan diserahkan ke bagian PPC untuk pembuatan nota. Setelah terjadi kesepakatan antara pelanggan dan *sales*, maka bagian PPC akan membuat nota yang akan digunakan untuk mencatat keseluruhan data pesanan dari pelanggan. Nota tersebut akan dibuat 2 rangkap. Rangkap pertama akan diserahkan ke bagian gudang bahan baku dan rangkap kedua akan diserahkan kepada cabang perusahaan di mana label dipesan.

Setelah nota telah dibuat, maka bagian PPC akan menyerahkan laporan pada *production manager* agar label yang dipesan dapat segera diproduksi. *Production manager* akan memberi informasi dan instruksi pada bagian gudang bahan baku tentang pesanan label tersebut. Lalu bagian gudang bahan baku akan melakukan pengecekan ke gudang, apakah terdapat stok benang yang akan digunakan dalam percetakan label yang dipesan. Apabila stok benang habis, maka bagian *purchasing* akan melakukan *re-stock* barang yang telah habis. Lalu *production manager* akan memberikan instruksi pesanan kepada bagian produksi atas label yang dipesan. Setelah itu, bagian produksi akan melakukan pekerjaannya. Setelah barang selesai diproduksi, maka bagian *finishing* akan melakukan pengepakan/*packaging*. Dengan demikian, barang akan siap didistribusikan kepada pelanggan. Pendistribusian label yang dipesan akan dikirimkan ke cabang perusahaan di mana pelanggan memesan label tersebut. Dari cabang tersebut pesanan akan langsung dikirimkan kepada pelanggan, beserta nota pesanan atas label yang dipesan. Seluruh data penjualan label akan dicatat dan diproses oleh bagian *accounting*, lalu akan dijadikan laporan yang akan diserahkan kepada direktur.

Seluruh order pemesanan label dari pelanggan akan di-input ke dalam database perusahaan untuk disimpan sebagai laporan mengenai jumlah stok benang yang sering digunakan dan waktu proses memproduksi pesanan label, sehingga dapat dilakukan pengecekan bila terdapat kesalahan produksi.

Deskripsi Implementasi Teknologi Informasi

Setelah dibentuknya Divisi TI pada PTNL, maka Divisi IT mempunyai tugas dan tanggung jawab seperti menyimpan data-data perusahaan pelanggan; memelihara dan menjaga kelancaran TI perusahaan selama dalam kegiatan perusahaan, dengan menangani kesalahan-kesalahan yang berhubungan dengan bagian TI; serta merencanakan pengembangan TI yang baik bagi perusahaan.

TI yang dimiliki oleh PTNL saat ini meliputi infrastruktur, yang terdiri dari: *hardware*, *software*, jaringan, internet, dan intranet.

Hardware

Untuk mendukung aktivitas bisnisnya, maka diperlukan perangkat keras yang meliputi: 45 *personal computer* yang tersebar tiap fungsi bisnis. Untuk *user*, dengan spesifikasi Pentium 4, 2GHz, 1Gb RAM, 80 Gb HD, 10/100/1000 ethernet NIC dan Untuk *Data Center* mempunyai spesifikasi Pentium 4 2,2GHz, 4Gb RAM, 500Gb HD; *20 printer* yang digunakan untuk mencetak data dengan berbagai merk; *modem ADSL Link sys*; UPS (*Uninterruptible Power Supply); switch 28port D.Link/ 24port 3com; router wiFi Linksys; scanner; dan fax.*

Software

Perangkat lunak yang digunakan adalah: *user: Windows XP profesional* dan *server: Window server 2003 R2*; *SQL Server 2005 standard edition*; *antivirus* menggunakan *Sophos-antivirus*; *Microsoft Office* 2003, *Open Office.org3, IBM Lotus Notes 8.5*; *Microsoft Visual Studio* 2008. Bagian

pada *software* ini yang dipakai adalah Vb.net (untuk *desktop*), Asp.net (untuk aplikasi berbasis *web*), C# (untuk *library*), dan juga PHP (untuk internet).

Jaringan

Untuk menghubungkan pemrosesan transaksi antar PC digunakan Wireless LAN (*Local Area Network*) dan yang menghubungkan antar perusahaan dari cabang ke pusat menggunakan *Citrix*.

Internet

Untuk koneksi internet menggunakan Telkom Speedy.

Intranet

Adapun kondisi dari *hardware* seperti *monitor, keyboard*, *mouse*, dan *printer* masih dalam kondisi yang baik dan masih dapat digunakan untuk 5 tahun ke depan. Keluhan yang sering muncul bukan pada perangkat TI, melainkan pada kesalahan yang dilakukan *user* dalam menginputkan transaksi (*Human Error*). Masalah lain yang muncul adanya virus-virus yang memasuki sistem yang mengganggu jaringan. Bagian TI juga senantiasa meng-*update antivirus* dan melakukan *maintenance* TI.

Perusahaan menerapkan pencatatan keuangan untuk pengeluaran bagian TI sebagai beban operasional yang menjadi satu dengan beban operasional perusahaan, sehingga tidak ada pencatatan khusus untuk pengeluaran TI. Oleh sebab itu, akan sulit untuk dilakukan penelusuran atas pengeluaran biaya yang dilakukan bagian TI dalam memperlancar proses bisnis PTNL.

PEMBAHASAN

Dalam pengukuran risiko yang dilakukan pada PTNL, kami telah mengumpulkan dan mengolah data berdasarkan kuisioner yang telah dibagikan kepada Bapak Johan selaku manajer TI dan juga para staf-staf TI lainnya. Kuisioner yang dibagikan digunakan untuk mengetahui kelemahan dari hasil pengukuran risiko serta mencari solusi atas risiko-risiko yang terjadi dalam PTNL. Kuisioner yang dibuat dengan menggunakan metode OCTAVE-S terdiri dari 3 tahap, yaitu: membangun aset berbasis profil ancaman, mengidentifikasi kerentanan infrastruktur, serta mengembangkan strategi keamanan dan perencanaan. Dari ketiga tahap ini, dijabarkan menjadi 5 proses yang terdiri dari 16 aktivitas dan 30 langkah.

PTNL saat ini memiliki reputasi yang baik. Hal ini dapat dilihat dari kehilangan pelanggan sebesar 3 persen per tahun. Ini membuktikan bahwa terdapat kesetiaan pelanggan dalam menggunakan jasa perusahaan. Angka tersebut berbanding jauh dengan penambahan pelanggan pada perusahaan selama tahun 2008 ini yang mencapai 10 persen.

Dari segi finansial perusahaan, biaya operasional perusahaan dikategorikan sedang karena meningkat 10 persen. Dengan demikian kehilangan pendapatan akan berkurang seiring biaya operasional yang meningkat. Kehilangan pendapatan tersebut diperkirakan sekitar 15 persen. Biaya operasional ini dihabiskan hampir 40 persen untuk kebutuhan TI organisasi. Hal ini dikarenakan perombakan total perusahaan pada awal 2008.

Pelanggan yang bertambah mengakibatkan meningkatnya jam kerja untuk menunjang produktivitas perusahaaan. Pada 2008, produktivitas perusahaan bertambah sebesar 20 persen, dan diprediksikan akan terus meningkat sepanjang periode 2009.

Perlindungan kesehatan setiap karyawan menjadi tanggungan perusahaan. Untuk masalah kesehatan karyawan, perusahaan memberikan kompensasi sesuai dengan kebijakan yang diterapkan. Ancaman keselamatan pada karyawan dikategorikan rendah karena tidak pernah terjadi ancaman yang berakibat fatal. Untuk hukuman denda memang diberlakukan di dalam perusahaan ini, tetapi hal tersebut semata hanya dilakukan dengan tujuan agar para karyawan dapat lebih mengedepankan kedisiplinan serta profesionalitas kerja.

PTNL juga memiliki 15 praktek keamanan, yang diantaranya meliputi sebagai berikut. Pertama adalah kesadaran keamanan dan pelatihan. Dalam perusahaan ini sudah terdapat kesadaran anggota staf yang memahami dan mematuhi kebijakan keamanan, dengan menggunakan *password* yang baik dalam menggunakan sistem yang ada di perusahaan dan sudah terdapat dokumentasi dan verifikasi atas peraturan keamanan dan tanggung jawab yang harus dipatuhi staf. Tetapi dalam perusahaan ini, pelatihan hanya dilakukan untuk karyawan baru saja dan belum ada pelatihan yang dilakukan secara periodik. Hal ini menunjukkan kesadaran keamanan dan pelatihan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya pelatihan yang dilakukan secara periodik; bukan hanya untuk karyawan baru, tetapi untuk semua karyawan. Hal ini dilakukan supaya kesadaran keamanan karyawan menjadi meningkat.

Kedua adalah strategi keamanan. Strategi perusahaan telah secara rutin memasukkan pertimbangan keamanan dan kebijakan, serta strategi keamanan mempertimbangkan tujuan dan strategi bisnis perusahaan. Srategi pengamanan perusahaan telah berjalan dengan baik; tetapi dalam perusahaan ini, strategi pengamanan belum didokumentasikan dan dikaji secara rutin. Hal ini menunjukkan bahwa kesadaran keamanan dan pelatihan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah untuk membuat perubahan strategi bisnis perusahaan, harus ada dokumentasi dan dikaji secara rutin, agar karyawan dalam menjalankan strategi keamanannya menjadi lebih terarah.

Ketiga adalah manajemen keamanan. Dalam perusahaan ini, peraturan keamanan telah ditetapkan secara baik oleh perusahaan kepada semua karyawan, prosedur-prosedur manajemen keamanan telah didokumentasikan untuk mengawasi semua staf yang bekerja. Tetapi perusahaan ini belum mengalokasikan dana untuk pembiayaan aktivitas keamanan informasi, belum adanya proses yang formal dalam menilai dan mengelola risiko, belum terdapat mekanisme yang resmi dalam menyiapkan manajer dengan ringkasan informasi yang berhubungan dengan keamanan yang penting. Hal ini menunjukkan bahwa manajemen keamanan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah adanya pengalokasian dana dalam menjaga keamanan informasi, agar segala kerusakan yang muncul dapat segera ditangani; menyediakan proses yang formal dalam menilai dan mengelola risiko; serta menyediakan mekanisme resmi dalam menyiapkan manajer, dengan ringkasan informasi yang berhubungan dengan keamanan yang penting.

Keempat adalah kebijakan keamanan dan peraturan. Dalam perusahaan ini, terdapat peraturan dan kebijakan keamanan informasi, dan diterapkan oleh seluruh staf. Kebijakan tersebut secara berkala ditinjau dan diperbaharui. Tetapi, evaluasi yang dilakukan dalam perusahaan tidak didokumentasikan secara menyeluruh, untuk memastikan pemenuhan kebijakan keamanan informasi. Kesimpulannya adalah peraturan dan kebijakan keamanan perusahaan diperlukan sedikit perbaikan, tetapi tidak terlalu berarti (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya proses yang didokumentasi dalam setiap evaluasi yang dilakukan untuk pemenuhan kebijakan keamanan informasi, agar dapat diketahui setiap evaluasi yang dilakukan pada perusahaan.

Kelima adalah manajemen keamanan kolaboratif. Perusahaan telah membuat kebijakan dan prosedur untuk melindungi informasi milik perusahaan lain dalam prosedur

kolaborasi. Akan tetapi, tidak tersedia dokumentasi ataupun mekanisme formal terhadap setiap prosedur dan hasil yang ada (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya dokumentasi ataupun mekanisme formal terhadap setiap prosedur dan hasil yang ada.

Keenam adalah rencana *contingency*. Perusahaan ini telah mempunyai rencana cadangan yang disediakan untuk menangani kemungkinan buruk yang akan terjadi. Analisis, operasi, aplikasi, dan data yang penting telah dilakukan. Tetapi, belum semua staf menyadari perlunya rencana cadangan, rencana pemulihan bencana, dan rencana untuk menghadapi keadaan darurat. Perusahaan juga belum terdapat dokumentasi seluruh rencana cadangan dan rencana cadangan tersebut belum diuji tingkat keberhasilannya. Hal ini menunjukkan rencana cadangan dan pemulihan dari bencana perlu adanya perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah mendokumentasikan seluruh rencana cadangan untuk menganggapi keadaan darurat menjadi jelas dan mudah untuk diikuti oleh karyawan; serta menguji tingkat keberhasilan rencana cadangan agar keberhasilan dari rencana cadangan tersebut lebih akurat.

Ketujuh adalah pengendalian akses fisik. Perusahaan telah mempunyai pengendalian akses fisik yang baik. Dapat dilihat dari rencana keamanan fasilitas dan prosedur untuk menjaga lokasi, bangunan, dan area apapun yang dibatasi telah didokumetasi. Terdapat kebijakan untuk mengendalikan akses fisik ke tempat kerja serta *hardware* dan *software*. Contohnya adalah area bangunan dan tempat kerja, serta tempat server hanya dapat dimasuki oleh orang yang berwenang. Kesimpulannya adalah pengendalian akses fisik dalam perusahaan sudah baik (*Stoplight status GREEN*).

Kedelapan adalah Pemantauan dan Audit Keamanan Fisik. Perusahaan telah melakukan hal yang baik dalam mengawasi dan mengaudit keamanan secara fisik. Dapat dilihat dari catatan pemeliharaan yang disimpan untuk mendokumentasi perbaikan dan modifikasi dari komponen fasilitas fisik. Tindakan individu atau grup berkaitan dengan media yang dikontrol dan secara fisik dapat dilaporkan. Adanya catatan audit dan pengawasan secara rutin diperiksa kejanggalannya. Kesimpulannya adalah pengendalian akses fisik dalam perusahaan sudah baik (*Stoplight status GREEN*).

Kesembilan adalah sistem dan manajemen jaringan. Dalam perusahaan telah terdapat *firewall* yang di-*update* secara rutin untuk menjaga sistem dan jaringan yang ada dalam perusahaan. Informasi sensitif yang ada dalam perusahaan telah di-*back up daily, weekly, monthly*. Semua sistem dalam perusahaan selalu *up to date* dengan direvisi dan di-*patch*. Perubahan terhadap *hardware* dan *software* direncanakan dan dikontrol. Jika dalam perusahaan terdapat sistem yang tidak diperlukan, maka akan segera dihapus. Dengan demikian, manajemen jaringan dan sistem terdapat beberapa kekurangan (*Stoplight status YELLOW*). Rekomendasinya adalah perlunya mendokumentasikan keseluruhan rencana keamanan utnuk menjaga sistem dan jaringan.

Kesepuluh adalah pemantauan dan audit keamanan TI. Dalam perusahaan ini, pengawasan sistem dan jaringan telah dilakukan secara rutin oleh perusahaan. *Firewall* dan komponen keamanan lainnya telah diaudit secara periodik untuk memenuhi persyaratan keamanan. Kesimpulannya adalah pengawasan dan pengauditan keamanan TI dalam perusahaan sudah baik (*Stoplight status GREEN*).

Kesebelas adalah pengesahan dan otorisasi. Perusahaan ini telah mempunyai akses kontrol sesuai akses dan otentikasi penggunaan, sesuai dengan kebijakan yang ada untuk membatasi akses pengguna. Dokumentasi kebijakan yang terdapat dalam perusahaan berguna untuk membuat dan mengakhiri hak untuk mengakses informasi. Contohnya adalah adanya *id* dan *password* untuk setiap masing-masing *user*. Metode atau mekanisme yang disediakan untuk memastikan bahwa informasi yang sensitif tidak diakses, diubah ataupun dihancurkan secara tidak sah. Metode atau mekanisme secara periodik ditinjau ulang dan diverifikasi. Kesimpulannya adalah otentikasi dan otorisasi dalam perusahaan sudah baik (*Stoplight status GREEN*).

Keduabelas adalah manajemen kerentanan. Dalam perusahaan terdapat prosedur keamanan kerentanan yang telah diikuti dan secara periodik ditinjau, serta terdapat penilaian kerentanan teknologi dan kerentanan dihadapi ketika risiko teridentifikasi. Dengan demikian, manajemen kerentanan terdapat beberapa kekurangan yang tidak terlalu signifikan (*Stoplight status YELLOW*). Rekomendasinya adalah mendokumentasikan seluruh dokumentasi untuk mengelola kerentanan.

Ketigabelas adalah enkripsi. Perusahaan telah mengontrol keamanan yang sesuai untuk melindungi informasi yang sensitif selama dalam penyimpanan, misalnya enkripsi data. Enkripsi data dalam perusahaan telah dilakukan dengan baik. Kesimpulannya adalah enkripsi dalam perusahaan sudah baik (*Stoplight status GREEN*).

Keempatbelas adalah desain dan arsitektur keamanan. Sebelum membuat arsitektur dan desain untuk sistem yang baru, perusahaan telah mempertimbangkan strategi keamanan, kebijakan dan prosedur, sejarah keamanan, serta hasil dari penilaian risiko keamanan. Akan tetapi, perusahaan tidak mempunyai diagram *up to date* yang menunjukkan keamanan arsitektur dan topologi jaringan dari perusahaan. Dengan menggunakan diagram *up to date*, lebih mudah dilihat bagaimana perkembangan keamanan perusahaan. Hal ini menunjukkan arsitektur keamanan dan desain dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah adanya diagram *up to date* untuk menunjukkan bagaimana gambaran perusahaan dalam segi perancangan dan arsitektur keamanan.

Kelimabelas adalah manajemen insiden. Perusahaan telah mengikuti prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dengan baik. Tetapi perusahaan belum terdapat dokumentasi atas prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dan pelanggaran. Dalam hal ini, manajemen insiden dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya dokumentasi atas prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dan pelanggaran.

Hasil Identifikasi dan Analisis

Dampak ancaman melalui akses jaringan yang dilakukan oleh internal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi bernilai sedang untuk penyingkapan dan interupsi, dan bernilai tinggi untuk modifikasi dan penghancuran; dampak terhadap finansial pada hasil penyingkapan, modifikasi, dan interupsi bernilai sedang, untuk penghancuran bernilai tinggi; dampak terhadap produktifitas bernilai sedang untuk penyingkapan dan modifikasi, dan tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda bernilai sedang untuk semua hasil ancaman, sedangkan untuk dampak terhadap perlindungan bernilai rendah.

Dampak ancaman melalui akses jaringan yang dilakukan oleh internal perusahaan secara sengaja adalah: dampak terhadap reputasi bernilai sedang untuk semua hasil ancaman, sedangkan terhadap finansial bernilai tinggi pada keseluruhan hasil ancaman; dampak terhadap produktifitas bernilai rendah untuk penyingkapan, sedang untuk modifikasi, dan tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda bernilai sedang untuk semua hasil ancaman dan dampak terhadap perlindungan bernilai rendah juga untuk semua hasil ancaman.

Dampak ancaman melalui akses jaringan yang dilakukan oleh eksternal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi bernilai sedang untuk penyingkapan dan modifikasi, dan bernilai rendah untuk penghancuran dan interupsi; dampak terhadap finansial

bernilai sedang untuk hasil interupsi, dan bernilai tinggi untuk hasil penyingkapan, modifikasi dan penghancuran; dampak terhadap produktifitas bernilai rendah untuk hasil penyingkapan, bernilai sedang untuk hasil modifikasi dan bernilai tinggi untuk hasil penghancuran dan interupsi; serta dampak terhadap denda dan perlindungan masing-masing bernilai sedang dan rendah untuk semua hasil ancaman.

Dampak ancaman melalui akses jaringan yang dilakukan oleh eksternal perusahaan secara sengaja adalah: dampak terhadap reputasi dan finansial, masing-masing bernilai rendah dan tinggi untuk semua hasil ancaman; dampak terhadap produktifitas bernilai rendah untuk penyingkapan, bernilai sedang untuk modifikasi dan bernilai tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda dan perlindungan, sama dengan sebelumnya yaitu masing-masing bernilai sedang dan rendah untuk semua hasil ancaman.

Dampak ancaman melalui akses fisik yang dilakukan oleh internal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi, finansial dan denda, bernilai sama yaitu sedang untuk semua hasil ancaman, sedangkan dampak terhadap produktifitas dan perlindungan bernilai rendah untuk semua hasil ancaman.

Dampak ancaman melalui akses fisik yang dilakukan oleh internal perusahaan secara sengaja adalah: dampak terhadap reputasi, finansial dan denda bernilai sedang pada semua hasil ancaman, sedangkan untuk perlindungan bernilai rendah; serta dampak pada produktifitas bernilai sedang untuk hasil modifikasi dan penyingkapan, dan bernilai tinggi untuk hasil modifikasi dan interupsi.

Dampak ancaman melalui akses fisik yang dilakukan oleh eksternal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi, finansial dan denda bernilai sedang untuk semua hasil ancaman, sedangkan dampak terhadap produktifitas dan perlindungan bernilai rendah untuk semua hasil ancaman.

Dampak ancaman melalui akses fisik yang dilakukan oleh eksternal perusahaan secara sengaja adalah: dampak terhadap reputasi, finansial, dan produktifitas bernilai sedang untuk semua hasil ancaman sedangkan dampak terhadap denda dan perlindungan bernilai rendah untuk semua hasil ancaman.

Rencana Mitigasi

Area Mitigasi (Kesadaran Keamanan dan Pelatihan)

Aktivitas mitigasinya adalah menyediakan pelatihan kesadaran keamanan untuk seluruh karyawan secara periodik (2 kali dalam 1 tahun), menyediakan mekanisme resmi untuk menyiapkan panduan keamanan yang di-*update* secara periodik. Alasannya adalah agar karyawan lebih menyadari dan tidak melupakan pentingnya keamanan, agar anggota karyawan dapat mengikuti perkembangan masalah keamanan yang baru. Yang bertanggung jawab dalam area mitigasi ini adalah Divisi TI. Dukungan tambahan yang diperlukan dalam area ini adalah Manajer TI harus mendukung aktivitas ini, dengan cara menentukan jadwal yang pasti untuk pelatihan kesadaran keamanan. Perusahaan memberikan dukungan berupa dana untuk pelatihan tersebut. Perusahaan juga membuat peraturan untuk diadakannya *meeting* jika ada masalah keamanan yang baru atau yang akan diperiodik.

Area Mitigasi (Strategi Keamanan)

Aktivitas mitigasinya adalah perusahaan harus mendokumentasikan strategi, tujuan, dan sasaran keamanan. Alasannya adalah agar karyawan, dalam menjalankan strategi keamanannya menjadi lebih terarah. Yang bertanggung jawab dalam area ini adalah Divisi TI. Dukungan tambahan untuk area ini adalah manajer TI menunjuk satu tim untuk mendokumentasikan strategi, tujuan, dan sasaran keamanan.

Area Mitigasi (Rencana Cadangan atau Pemulihan Bencana)

Aktivitas mitigasinya adalah mendokumentasikan seluruh rencana cadangan, rencana pemulihan bencana, dan rencana kemungkinan untuk menanggapi keadaan darurat, menguji rencana cadangan, rencana pemulihan bencana, dan rencana kemungkinan untuk menanggapi keadaan darurat secara resmi. Alasannya adalah agar rencana cadangan, rencana pemulihan bencana, dan rencana kemungkinan untuk menanggapi keadaan darurat menjadi lebih jelas dan lebih mudah untuk diikuti oleh karyawan, untuk memastikan tingkat keberhasilan rencana cadangan, rencana pemulihan bencana, dan rencana kemungkinan untuk menanggapi keadaan darurat dengan lebih akurat. Yang bertanggung jawab adalah Divisi TI. Dukungan tambahan yang diperlukan meliputi Manajer TI menunjuk satu tim untuk mendokumentasikan rencana cadangan, rencana pemulihan bencana, dan rencana kemungkinan, serta Manajer TI melakukan pengujian dengan cara membuat skenario rencana.

Area Mitigasi (Manajemen Keamanan)

Aktivitas mitigasinya adalah menyediakan anggaran perusahaan secara khusus dalam pembiayaan untuk aktivitas keamanan informasi, menyediakan proses yang formal dan dokumentasi dalam menilai dan mengelola risiko keamanan informasi, menyediakan mekanisme resmi dan dokumentasi untuk menyiapkan manajer dengan ringkasan informasi yang berhubungan dengan keamanan yang penting. Alasannya adalah agar segala kerusakan yang muncul dapat segera ditangani, proses yang formal dan dokumentasi dalam menilai dan mengelola resiko keamanan informasi diperlukan untuk berjaga-jaga apabila risiko terjadi pada saat Divisi TI sedang tidak ditempat, maka staf lain dapat mengambil langkah-langkah dalam mengatasi risiko tersebut dengan melihat dokumentasi tersebut sebagai panduan, agar ringkasan yang dihasilkan untuk manajer lebih lengkap dan tepat. Yang bertanggung jawab adalah Divisi IT. Dukungan tambahan yang diperlukan adalah Direktur memberikan dukungan dengan memberikan dana untuk menambah anggaran perusahaan, Manajer TI menyediakan proses dan mendokumentasikan proses tersebut secara jelas, dan Manajer TI menyediakan mekanisme yang resmi dan didokumentasikan.

PENUTUP

Dari hasil analisis yang dilakukan, maka ada beberapa hal yang dapat disimpulkan, yaitu: secara garis besar manajemen risiko pada PTNL sudah berjalan dengan baik, hanya terdapat beberapa kelemahan yang harus diperbaiki untuk menunjang kinerja perusahaan agar lebih maksimal dan efektif; dalam hal keamanan informasi, PTNL masih memiliki sedikit kekurangan, khususnya risiko-risiko yang melalui akses jaringan karena pengamanan perusahaan melalui jaringan masih kurang terorganisir dengan baik; praktek keamanan dalam perusahaan telah diterapkan dengan cukup baik karena hanya terdapat beberapa kekurangan dari 15 praktek keamanan yang dievaluasi; serta diperlukan pelatihan karyawan secara menyeluruh pada setiap bagian/ divisi dalam setiap periodik.

DAFTAR PUSTAKA

Alberts, C, et al. (2005). *Introduction to OCTAVE-S*. U.S. Patent & Trademark Office. United State: Carnegie Mellon University.

Bandyopadhyay, K. et al. (1999). *Management Decision*, Vol. 37, hlm. 437. London.

Djojosoedarso, S. (2005). *Prinsip-prinsip Manajemen Risiko Asuransi*, Edisi revisi. Jakarta: Salemba Empat.

Febrian, Jack. (2000). *Kamus Komputer dan Istilah TI*.
Gondodiyoto, S., dan Hendarti, H. (2006). *Audit Sistem Informasi*. Jakarta: Mitra Wacana Media.
Haag, Cummings, dan Cuberry, C. (2005). *Management Information Systems for the Information Age*, Edisi kelima. New York: McGraw-Hill.
Hughes, G. (2006). *Five Steps to IT Risk Management Best Practices*. Risk Management, Vol. 53, hlm. 7, 34.
Jordan, E., dan Silcock, L. (2005). *Beating IT Risks*. England: John Wiley and Sons, Inc.
McLeod, R., dan Schell, G. P. (2007). *Management Information Systems,* Edisi kesepuluh. New Jersey: Pearson Prentice Hall.
Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Washington D.C: Auerbach/CRC Press Release.
Turban, Efraim. et.al. (2003). *Introduction to Information Technology*, 2th edition. England: John Wiley and Sons, Inc.