BAB V

HASIL DAN PEMBAHASAN

5.1 Analisis Penilaian dan Identifikasi Risiko Keamanan *Supply Chain*

Pada tahap awal perumusan skenario yang telah dirancang tentang ancaman keamanan, sebelumnya telah dilakukan terlebih dahulu penilaian keamanan di PT. Pos Indonesia Yogyakarta. Peneliti melakukan beberapa pengkajian kinerja perusahaan pada tabel 4.1 berdasarkan ISO 28001:2007 dalam proses mengidentifikasi risiko keamanan yang berpotensi mengancam aktivitas *supply chain* perusahaan. Kajian kinerja menguraikan kontrol yang seharusnya dimiliki perusahaan tersebut. Daftar kajian kinerja diklasifikasikan menjadi lima aspek sesuai dengan ruang lingkup keamanan perusahaan yang ada di PT. Pos Indonesia Yogyakarta

5.1.1 Manajemen Keamanan Rantai Pasok

Bedasarkan hasil wawancara dan obeservasi yang sudah dilakukan, PT. Pos Indonesia Yogyakarta memiliki jaringan *supply chain* yang memiliki beberapa tahapan alur yang sangat panjang hingga sampai ketangan penerima/konsumen. Namun, PT. Pos Indoensia Yogyakarta ini belum memiliki individu yang bertanggung jawab akan manejemen sistem keamanan *supply chain* perusahaan. Dan perusahaan ini belum memiliki penagnggung jawab pengolahan manajemen risiko yang teridentifikasi sangat berpotensi mengalami ancaman perusahaan

5.1.2 Rencana Keamanan

Untuk rencana keamanan perusahaan sudah menerapkan sistem keamanan untuk menjaga setiap aktivitas *supply chain.* Perusahaan sudah mempunyai beberapa rencana sistem keamanan mulai dari keamanan organisasi mitra agen yang ada diseluruh daerah Yogyakarta, melakukan rencana manajemen kritis, kelanjutan bisinis dan rencana

pemulihan keamanan yang bertujuan untuk meningkatkan keuntungan perusahaan dan sistem keamanan yang bagus sehingga PT. Pos Indonesia Yogyakarta ini dapat dipercaya oleh konsumen.

5.1.3 Keamanan Aset

PT. Pos Indonesia Yogyakarta memiliki lahan yang sangat luas dan memiliki bangunan-bangunan dan benda-benda yang mudah terbakar. Dengan area yang sangat luas tersebut, perusahaan sudah memiliki beberapa perangkat yang sangat membantu menangani masalah keamanan fisik gedung perusahaan. Perusahaan juga menyediakan APAR pada beberapa titik di setiap departemen yang ada pada perusahaan tersebut. Namun, dengan disediakannya APAR tidak menutupi kemungkinan terjadi kebakaran pada area gedung. Hal ini dikarenakan tidak setiap individu dapat menggunakan APAR hanya beberapa pekerja yang dapat menggunakan benda tersebut.

Perusahaan memiliki beberapa syarat untuk melakukan pengendalian akses bagi tamu atau pengunjung. Namun akses tersebut jika sudah diijinkan oleh pihak manajemen yang bertanggung jawab atas tamu atau pengunjung, keluar masuknya tamu/pengunjung tidak akan di cek lagi oleh sekuriti yang menjaga. Jika terjadi pelanggaran oleh para tamu atau pegawai yang tidak seharusnya dilakukan maka petugas keamanan akan menindak lanjuti masalah tersebut dengan kepolisian yang ada di yogkayakarta

Perusahaan sudah memiliki beberapa CCTV yang ada pada setiap area yang penting mulai dari setiap ruangan gedung, lorong gedung, dan area proses pengiriman. Dan setiap rekaman yang pada penyimpanan CCTV tidak ada batas waktu penghapusan. Sudah terdapat individu yang bertanggung jawab terkait penyimpanan barang di gudang proses dan pengiriman oleh petugas keamanan

5.1.4 Keamanan personel

Keamanan personel merupakan tanggungjawab perusahaan yang dimana seluruh kegiatan yang dilakukan oleh karyawan di kantor atau di gedung proses pengiriman adalah tanggung jawab *top Management.* Keterlibatan dan komitmen karyawan adalah vital bagi suksesnya keamanan. Karyawan perlu ditumbuhkan kepeduliannya terhadap efek dari manajemen keamanan terhadap kualiatas lingkungan kerjanya dan harus didukung dengan secara aktif berkontribusi pada manajemen keamanan. Karyawan tidak mungkin dapat membuat kontribusi yang efektif pada manajemen keamanan kecuali jika mereka mengerti akan kebijakan keamanan perusahaan tersebut. Kebijakan-kebijakan yang diterapkan oleh PT. Pos Indonesia Yogyakarta yaitu evaluasi keamanan pada waktu pagi dan malam hari namun tidak ada evaluasi karyawan sesudah dan sebelum melakukan pekerjaan untuk diterapkannya keamanan tersebut. Selain itu juga, pelatihan pekerjaan telah diterapkan oleh perusahaan untuk memberikan pengetahuan/*jobdesc* sesuai dengan pekerjaan yang mereka lakukan. Untuk pelatihan khusus keamanan perusahaan belum menerapkan prosedur tersebut. Dan tidak ada pemberitahuan secara tertulis oleh *Top Management* mengenai keryawan yang sudah non aktif dalam pekerjaannya sehingga bisa saja menimbulkan risiko ancaman keamanan internal.

Tingkat keamanan personel juga rendah ketika kargo barang yang datang dalam area gedung tidak dijaga ataupun di cek setiap sudut kargo mobil, sehingga proses ini rentan untuk terkena ancaman keamanan. Keamanan personel yang berkaitan dengan kecelakaan kerja baik diarea gedung proses maupun kecelakaan karyawan diluar area perusahaan, karyawan yang bekerja di perusahaan PT. Pos Indonesia Yogyakarta mendapat jaminan asuaransi ketanagakerjaan berupa BPJS. Sehingga karyawan yang mengalami kecelakaan atau sakit bisa menggunakan asuransi tersebut.

5.1.5 Keamanan Informasi

Untuk keamanan informasi perusahaan semua prosedur yang dijalankan oleh setiap pegawai sudah sesuai dengan SOP yang diberikan sehingga proses pengiriman dilakukan dengan tepat waktu dari pengambilan barang kiriman, penerimaan barang

sampai barang tersebut ketangan konsumen sehingga informasi-informasi yang valid bisa langsung diproses oleh pihak perusahaan. Untuk barang-barang yang masuk ke area gudang proses sudah dilakukan proses pengecekan *manifest* setiap tujuan yang akan dikirim sehingga tidak ada barang-barang yang akan salah dikirim. Data-data informasi sudah di *back-up* oleh pihak IT jika terjadi kesalahan informasi atau ancaman-ancaman dari *eksternal* data tersebut tidak akan hilang. Namun pengendalian akses masih kurang dikarenakan setiap akses user tidak dilengkapi sistem pengolahan *password* sehingga perlindungan keamanan bisa di bobol oleh pihak-pihak yang tidak bertanggung jawab dan bisa saja penyalahgunaan informasi dapat terbongkar oleh pihak *internal.*

5.1.6 Keamanan Barang dan *Conveyance*

Terkait dengan keamanan barang dan *conveyance*, perusahaan sudah memiliki prosedur untuk membatasi ,mendeteksi dan melaporkan akses yang tidak sah untuk memasuki semua area gudang barang, dan keamanan peralatan perusahaan. Namun area akses untuk masuk kedalam area perusahaan tidak ada penjagaan dan begitu saja keluar dan masuknya transportasi dari luar. Untuk kegiatan pengiriman penanggung jawab sudah dilakukan oleh departemen distribusi yang diaman semua bentuk kegiatan pengiriman mulai dari pengiriman kota Yogyakarta hingga luar kota Yogyakarta selalu *stand by.* Sedangkan untuk pengawasan barang-barang kiriman yang ilegal dan dicurigai sebagai barang yang berbahaya, badan pengawasan sudah melakukan prosedur untuk melakukan panggilan kepada penegak hukum utuk ditindak lanjuti. Untuk semua rute perjalan oleh pihak pengantaran tidak ada prosedur atau panduan untuk rute tersebut, namun hanya terdapat prosedur kesepakatan untuk tenggat waktu pengiriman.

5.1.7 Keamanan Unit Transportasi Kargo Tertutup

Keamanan unit transportasi kargo tertutup sudah ada prosedur terdokumentasi untuk pemasangan dan pencatatan segel pengamanan mekanis sehingga barang-barang yang rusak atau segel mengalami rusak akan dimuat dalam berita acara dan segara dilakukan penanganan secepatnya. Setiap pengangkutan kargo tertutup akan selalu diadakan inspeksi oleh pihak keamanan transportasi agar ancaman-ancaman yang dari luar bisa

teratasi dan untuk menghindari juga kontaminasi barang ilegal yang dilakukan sebelum penyusunan kargo untuk memeriksa keutuhan fisik kargo. Dan tujuh proses inspeksi yang dianjurkan sudah diterapkan oleh perusahaan.

5.2 Analisis Daftar Risiko Keamanan *Supply Chain*

Setiap risiko diidentifikasi dari kontrol yang sudah dimiliki perusahaan berdasarkan kajian kinerja dengan membuat daftar skneario anacaman risiko. Identifikasi risiko dilakukan berdasarkan seluruh aktivitas mulai dari *inbound* hingga *outbound* perusahaan yang melibatkan pihak *eksternal*. Setelah merumuskan proses bisnis perusahaan, kemudian dilakukan penetapan ruang lingkup penilaian keamanan menurut ISO 28001:2007 yang meliputi beberapa objek terkait keamanan *supply chain* yaitu:

1. Keamanan aset
2. Keamanan personel
3. Keamanan barang dan *conveyance*
4. Keamanan informasi
5. Keamanan kargo tertutup

Identifikasi risiko dilakukan dengan wawancara kepada *expert*. Dari proses identifikasi diperoleh 23 daftar ancaman keamanan pada *supply chain* perusahaan seperti tertera pada tabel 4.2, dengan 4 risiko keamanan aset, 6 risiko keamanan personel, 6 risiko keamanan barang dan *conveyance*, 3 risiko keamanan informasi dan 4 keamanan unit kargo tertutup.

Setiap risiko yang telah teridentifikasi oleh ancaman penyebab dan sumber risikonya. Setelah dilkukan penilaian risiko berdasarkan tingkat keumungkinan dan dampak yang ditimbulkan akibat risiko tersebut sehingga dapat diperoleh skor dari setiap risiko. Tingkat kemungkinan dan dampak risiko didapatkan berdasarkan expert judgement sebagai *risk owner*. Dari perolehan skor tersebut kemudian dipetakan pada peta risiko untuk mengetahui prioritas dan kondisi dari masing-masing risiko dan dilakukan evaluasi pencegahan yang sesuai dengan masing-masing risiko.

5.3 Analisis Penilaian Risiko Keamanan *Supply Chain*

Sebelum dilakukan penilaian risiko keamanan, terlebih dahulu menentukan dampak dan kemungkinan terjadinya risiko dalam skenario ancaman keamanan. Kriteria dampak dan kemungkinan diperoleh berdasarkan hasil wawancara dengan *expert* dan observasi lapangan.

Kriteria dampak terbagi menjadi 8 kriteria yaitu dampak terhambatnya proses pengiriman, kerugian finansial, penurunan efektivitas kerja, ketidakpercayaan konsuumen, jadwal pengiriman yang tidak sesuai dan kemungkinan barang bisa terjadi kerusakan, pencurian dialamat rumah, kondisi kecelakaan, dan keterlambatan proses pengiriman. Setiap kriteria diuraikan dalam lima level yaitu sangat rendah, rendah, sedang, tinggi dan sangat tinggi. Selanjutnya pada setiap risiko yang teridentifikasi, diuraikan dampak yang didapat dari risiko tersebut, lalu ditentukan level konsekuensi dari dampak tersebut . Terdapat 1 risiko dengan level 4 yaitu tinggi.

Setelah mengetahui kriteria dampak risiko keamanan pada tabel 4.4, kemudian melakukan penentuan kemungkinan kejadian pada tabel 4.5 dimana kemungkianan tersebut terbagi menjadi 5 level skor yaitu *rare* (hampir tidak pernah terjadi), *unlikely* (bisa/mungkin terjadi), *moderate* (jarang terjadi), *likely* (sering terjadi), dan *almost certain* (hampir pasti selalu terjadi). pada setiap risiko yang ada, diuraikan kemungkinan kejadian dari risiko tersebut , lalu ditentukan skor kemungkinan. Penentuan kemungkinan kejadian dilakukan dengan mempertimbangkan kontrol yang telah dilakukan perusahaan.

Pada risiko keamanan penilaian dilakukan dengan melakukan fungsi perkalian antara konsekuensi dengan kemungkinan, satu per satu risiko kejadian yang ada. Lalu setelah didapatkan skor atau level risiko, nilai tersebut akan diklasifikasikan sesuai dengan kategori yaitu *insignificant, minor, moderate, major* dan *extreme.* Pembagian kategori ini akan digunakan dalam menentukan posisi risiko pada peta risiko. Peneliti mendapatkan masing-masing 3 risiko kategori *insignificant,* 8 risiko kategori *minor,* 12 risiko kategori *moderate,* 1 risiko kategori *major.*

5.4 Analisis Evaluasi Risiko Keamanan *Supply Chain*

Pada hasil tahap evaluasi risiko yaitu *risk map* sebelum mitigasi seperti pada gambar 4.14. Setiap warna pada peta risiko memiliki arti yang berbeda-beda. Warna hijau berarti risiko tingkat sangat rendah dan rendah (*insignificant* dan *minor*), warna kuning berarti risiko tingkat sedang (*moderate*), warna jingga berarti risiko tingkat tinggi (*major*) dan warna merah berarti risiko tingkat sangat tinggi (*extreme*). dari hasil pemetaan risiko keamanan diperoleh 3 risiko kategori *insignificant*, 8 risiko kategori *minor*, 12 risiko kategori *moderate*, 1 risiko kategori *major*.

Mitigasi merupakan langkah atau tindakan dalam penanganan risiko. Bentuk penceegahan dirumuskan berdasarkan pada tiga sumber yaitu lembaga sertifikasi profesi manajemen risiko (LSPMR), dan kuadaran pemetaan level risikoterdapat tindakan-tindakan yang dapat dilakukan untuk menangani risiko. Nilai risiko yang mendapatkan kuadaran I (*accept*) masuk kedalam batas toleransi risiko, sehingga risiko dapat diterima dan tidak dibutuhkan tindakan penanganan. Pada penelitian ini dilakukan mitigasi pada 13 risiko yang berada diluar batas toleransi, namun prioritas utama yaitu yang memiliki risiko yang tinggi yaitu sebagai berikut:

1. Sistem Informasi ERP eror dan tidak dapat di operasikan dengan skor 10

Satu risiko yang memiliki nilai tinggi masuk kedalam kategori keamanan informasi. Untuk keamanan informasi di PT. Pos Indonesia Yogyakarta ini belum memiliki rancangan khusus untuk melindungi data-data rahasia konsumen sehingga bisa saja terjadi kecurangan oleh pihak internal ataupun eksternal. Dan kesalahan-kesalahan saat mengkonfirmasikan barang masuk dan barang keluar sering terjadi sehingga barang-barang yang akan dikirim mengalami keterlambatan proses pengiriman. Maka dari itu pihak-pihak yang bertanggung jawab atas sistem operasi keamanan informasi harus ditingkatkan dan perlu adanya evaluasi setiap karyawan IT yang menangani sistem jaringan tersebut.

5.5 Analisis Mitigasi Risiko Keamanan *Supply Chain*

Mitigasi dilakukan bentuk sebagai pencegahan risiko. Pada Tabel 4.10 diusulkan mitigasi berdasarkan tiga perlakuan yaitu action yang bersumber dari Lembaga

Sertifikasi Profesi Manajemen Risiko (LSPMR), upaya pencegahan bersumber dari ISO 28001:2007, dan Pemetaan Level Risiko berdasarkan kuadran risiko. Tiga sumber diberlakukan agar peneliti dapat mengusulkan mitigasi yang lebih tepat sasaran. Kemudian, berdasarkan Tabel 4.11 diusulkan mitigasi risiko terhadap 13 risiko yang memiliki nilai melebihi batas toleransi risiko dimana terdapat 1 risiko kategori *major* yang menjadi prioritas penangan risiko, yaitu:

1. Sistem Informasi ERP eror dan tidak dapat di operasikan dengan skor 10

   Risiko keamanan informasi yang sangat sering terjadi pada saat memasukan data-data konsumen sampai dengan kesalahan para petugas menginput sebuah data-data pemasukan barang atau keluarnya barang dan sering juga terjadinya sistem informasi ERP yang tidak dapat dioperasikan sehingga menyebabkan terhambatnya proses pengiriman barang yang dijalankan oleh pihak internal perusahaan. Hal ini bisa saja menurunkan ketidakkepercayan konsumen terhadap pelayanan jasa yang diberikan kepuasan pelanggan yang berkurang dan bisa saja jasa tersebut terlihat kurang oleh para konsumen. Sebagai upaya untuk memberikan kepuasan pelayan jasa, Maka dari itu pihak-pihak yang bertanggung jawab atas sistem operasi keamanan informasi harus ditingkatkan dan perlu adanya evaluasi setiap karyawan IT yang menangani sistem jaringan tersebut dan memberikan lagi arahan-arahan yang bermanfaat bagi karyawan.

Berdasarkan uraian tindakan pencegahan tersebut, PT. Pos Indonesia Yogyakarta harus lebih memperhatikan dan memperbaiki sistem manajemen keamanan *supply chain* dari internal perusahaan terutama terkait keamanan informasi perusahaan, agar risiko-risiko yang mungkin terjadi dapat diminimalkan atau bahkan dihilangkan. Adanya organisasi pengelolaan risiko keamanan dalam perusahaan sangat diperlukan perusahaan, mengingat alur perpindahan barang yang sangat panjang hingga sampai ke tangan konsumen akan memicu munculnya potensi bahaya dalam proses *supply chain.*

Selanjutnya, setelah didapatkannya penanganan risiko pada 13 risiko di luar batas toleransi dengan prioritas 1 risiko kategori *major*, kemudian membuat rancangan estimasi mitigasi meliputi jangka waktu pelaksanaan mitigasi dan target yang akan dicapai bagi risiko yang berada diluar batas toleransi.

5.6 Analisis Estimasi Mitigasi Risiko Keamanan *Supply Chain*

Tahap penjadwalan dan estimasi dilaksanakan terhadap risiko yang dilakukan tindakan mitigasi, dalam penelitian ini dilakukan pada risiko yang memiliki nilai risiko melebihi batas toleransi risiko yaitu sebanyak 13 risiko. Estimasi sebagai bentuk perkiraan yang dilakukan untuk memantau target mitigasi risiko sehingga dapat berjalan sesuai yang telah direncanakan oleh perusahaan. Estimasi dilakukan dengan mereposisi risiko pada peta risiko awal seperti pada Gambar 4.13, sehingga risiko berpindah ke dalam area batas toleransi

Pada Tabel 4.12 yang merupakan estimasi mitigasi, dijabarkan mengenai risiko disertai dampak, kemungkinan, dan level risiko awal. Kemudian, dirumuskan tindakan mitigasi atau pencegahan sesuai usulan dengan menyesuaikan kondisi risiko. Apabila risiko dilihat cukup membahayakan maka dapat diusulkan lebih dari satu tindakan mitigasi. Pada estimasi mitigasi juga terdapat rencana pelaksanaan meliputi jangka waktu penerapan mitigasi, dan target yang akan dicapai ketika menerapkan mitigasi. Setelah itu, nilai risiko setelah mitigasi dapat ditentukan dengan nilai perolehan yang lebih aman dari nilai sebelumnya. Berikut merupakan penjabaran estimasi mitigasi ketiga prioritas risiko tersebut.

Sistem Informasi ERP eror dan tidak dapat di operasikan dengan skor 10

Bentuk mitigasi yang dapat dilakukan adalah pengecekan sistem IT jaringan internet secara berkala dan operasi keamanan informasi harus ditingkatkan dan perlu adanya evaluasi setiap karyawan IT yang menangani sistem jaringan tersebut. Dengan diberi waktu 3 bulan diharapkan karyawan IT dapat menjalankan keamanan informasi dapat terkendali 100 % dan bisa menurunkan *risk level* yang semula dari skor 10 dapat turun mendapatkan skor 2 kategori *minor*.

Setelah mitigasi dilaksanakan, seluruh risiko mengalami perubahan posisi sesuai dengan estimasi nilai risiko setelah mitigasi. Pada Gambar 4.15, risiko mengalami perpindahan dari yang semula berada diluar batas toleransi menjadi berada didalam batas toleransi. Pada Gambar 4.16 menunjukkan 23 risiko sudah berada dalam batas toleransi yang artinya risiko sudah berada pada area yang aman. Untuk sembilan risiko kategori minor sejak pemetaan risiko awal, tidak dilakukan tindakan mitigasi dikarenakan risiko berada dalam batas toleransi dan dapat diterima perusahaan. Peta

risiko setelah mitigasi yang ditunjukkan pada Gambar 4.16 menunjukkan posisi risiko ketika PT. Pos Indonesia Yogyakarta telah melakukan tindakan mitigasi secara menyeluruh.