JUSTIFIKASI PENGEMBALIAN INVESTASI VERSUS PENGEMBALIAN INVESTASI KEAMANAN

Teddy Oswari
Staf Pengajar Fakultas Ekonomi Universitas Gunadarma
toswari@staff.gunadarma.ac.id

ABSTRAK

Pertengahan Tahun 1990-an, pembukaan dan resiko pada aset informasi perusahaan secara mudah dapat ditentukan karena jaringan perusahaan pada waktu itu tertutup untuk dunia luar. Infrastruktur jaringan dan protokol jaringan mempunyai pemilik, peralatan endpoint masih menggunakan dumb terminal dan aset informasi pada waktu itu tersentralisasi dan terkontrol secara ketat. Sekuritas fisik dan akses kontrol menjamin kepastian, integritas dan pengadaan.

Ketika jaringan perusahaan masih tertutup, model pengembalian investasi (ROI) dipakai untuk mengenal produk-produk sekuritas yang pengembaliannya dapat dibuktikan. Kelemahan diserang dan ancaman dapat segera dikenali karena berada pada jaringan tertutup. Jaringan perusahaan saat ini tidak lagi tertutup. Pengaksesan oleh pemakai, aplikasi dan komputer yang tidak dikenal sudah mulai diberikan izin. Pembukaan yang ditimbulkan oleh tamu yang tidak dikehendaki ini sangatlah sulit untuk dihitung.

Tulisan ini akan mendeskripsikan sebuah pendekatan baru pada sekuritas perusahaan menggunakan analisis Pengembalian investasi keamanan, sebuah perangkat yang efektif untuk mengidentifikasikan pengembalian dari penanaman modal pada sekuritas. Analisis Pengembalian investasi keamanan diharapkan akan dapat menghitung tingkat pengembalian dari penanaman modal pada sekuritas saat ini.

Kata kunci: Pengembalian investasi, Jaringan perusahaan, Pengembalian investasi keamanan

PENDAHULUAN

Pertengahan Tahun 1990-an, pembukaan dan resiko pada aset informasi perusahaan secara mudah dapat ditentukan karena perusahaan pada waktu itu tertutup untuk dunia luar. Infrastruktur dan protokol mempunyai pemilik, peralatan akhir masih menggunakan *dumb terminal* dan aset informasi pada waktu itu tersentralisasi dan terkontrol secara ketat. Sekuritas fisik dan akses kontrol menjamin kepastian, integritas dan pengadaan.

Saat ini, pada era teknologi seperti internet, tanpa kabel dan aplikasi yang memakai jaringan, manajer bisnis perusahaan menggunakannya untuk mencapai akses pasar global, pengurangan harga dan penambahan produktifitas. Teknologi ini, disamping menawarkan keuntungan yang besar, juga memiliki celah sekuritas. Jaringan perusahaan terbuka untuk akses yang tidak diundang seperti oleh pemakai, komputer dan aplikasi yang tidak dikehendaki. Mereka bisa terlepas dari otorisasi dan pro-

ses otentifikasi yang ditetapkan. Jaringan perusahaan pada saat ini biasa disebut dengan jaringan terbuka. Jaringan terbuka mengakibatkan setiap perusahaan yang memiliki akses internet untuk mengalokasikan sejumlah dana bagi sekuritas komputer perusahaannya. Investasi pada sekuritas merupakan langkah untuk memproteksi aset informasi perusahaan.

Selama bertahun-tahun perusahaan yang bergerak pada bidang Teknologi Informasi (TI) mengalami kesulitan dalam meyakinkan pihak manajemen bisnis perusahaan mengenai pembiayaan pada bidang teknologi informasi. Walaupun demikian, saat ini mereka sudah mulai mengenal masalah investasi dengan lebih baik, dimulai dengan menggunakan komputer yang lebih bagus, meningkatkan kemampuan server, menginstalasi jaringan lokal atau sebuah VPN. Hal tersebut terjadi karena manajer TI sudah dapat menghitung pengembalian moneter dari investasi semacam itu. Pada investasi untuk sekuritas tidaklah sesulit investasi pada kasus di atas, namun demikian masih merupakan hal yang sulit diterima. Kebanyakan orang berinvestasi pada sekuritas supaya tidak terkena serangan. Perilaku seperti itu akan menyulitkan bila ternyata anggaran yang dianggarkan pas-pasan.

PEMBAHASAN

Menyeimbangkan Resiko dan Upah

Pengembaiian investasi adalah generasi pengembalian, penghematan atau penambahan produktivitas. Dalam hal ini manajer TI dan pimpinan perusahaan harus dapat membuktikan pengembalian investasi (ROI) merupakan pengukuran preventif untuk pengeluaran modal, kemungkinan penambahan tenaga manusia yang bentuknya berupa sebuah kurva langkah pembelajaran.

Kebutuhan akan benteng, sebuah arsitektur jaringan yang aman, enkripsi, tanda tangan digital dan back up yang lebih baik dan kemampuan pemulihan, filtering, monitoring, deteksi intrusi (penyerangan)/ pencegahan dan kemampuan *single sign-on* adalah suatu keharusan. Setiap diskusi anggaran memerlukan sebuah tindakan seimbang dalam mempertimbangkan nilai dari sebuah produk atau layanan terhadap pengembalian investasi yang diharapkan. Dengan sekuritas, seringkali sulit untuk untuk mengukur pengembalian yang diharapkan sementara ongkos dapat digambarkan dengan sangat jelas, seperti biaya yang harus dikeluarkan untuk meng*install* perangkat lunak pengukur sekuritas.

Biro Federal Investigasi Amerika (FBI) melaporkan bahwa rata-rata kerugian pada tiap perusahaan dari pelanggaran sekuritas pada Tahun 2002 adalah 6,6 juta dollar Amerika. Jumlah tersebut menurun menjadi 2,7 juta dollar pada Tahun 2003, sebuah penurunan yang berarti, namun tetap saja sebuah kerugian yang harus dipertimbangkan bagi perusahaan untuk mengatasinya.

Tiga Model Untuk Menganalisis Investasi

Informasi pada organisasi sekuritas berada di bawah te-

kanan yang terus membesar untuk dapat mengidentifikasi pengembalian dari penanaman modal pada teknologi informasi termasuk investasi pada perangkat lunak sekuritas.

Terdapat tiga model yang digunakan untuk menganalisis investasi pada sekuritas:

1. *Best Practices*. Model ini menaksir kebutuhan sekuritas dengan mengidentifikasi aset yang harus diproteksi. Aset dapat meliputi sumber daya, sebuah desain produk, infrastruktur jaringan komputer, informasi kesehatan yang terpercaya, para pelanggan, pemasok, atau data pegawai. Kehilangan kepercayaan, integritas atau keberdayagunaan adalah nilai yang tidak dapat diukur, seperti pada sebuah kehilangan reputasi. Model ini berpegang pada bahwa pengeluaran untuk sekuritas harus dialokasikan agar sesuai atau melebihi standar industri.
2. Asuransi. Model ini memerlukan analisis yang luas dari kemudahan diserang, ancaman internal dan eksternal dan nilai dari semua aset informasi yang ada. Ancaman datang dalam bentuk yang bermacam-macam dan memiliki efek yang bermacam-macam. Bencana yang alami, masalah hukum, sabotase dan pencurian adalah bentuk dari ancaman. Kemudahan diserang adalah kelemahan atau faktor yang mengurangi ukuran sekuritas. Penjagaan yang aman pada saat ini digunakan untuk mengukur perkiraan kerugian tahunan. Investasi sekuritas dialokasikan untuk menghapus resiko, memperbaiki infrastruktur sekuritas, memindahkan resiko (membeli asuransi) atau menerima kekalahan (kehilangan).
3. Setelah mengidentifikasi aset, dan ancaman serta kelemahannya, lalu melakukan pertimbangan mengenai nilai total organisasi untuk seluruh waktu kehidupan dari aset. Menentukan nilai dari aset produksi, riset dan pengembangan dan keadaan kritis setiap aset bisnis. Kemudian setiap pelaku sekuritas haruslah memahami pentingnya langkah yang telah dilakukan untuk menentukan berapa kerugian perusahaan bila kehilangan dibandingkan berapa harganya bila diproteksi. Model pengembalian investasi keamanan mengandalkan dua komponen sebuah komponen asuransi untuk menganalisis resiko yang dikurangi oleh usulan investasi sekuritas dan sebuah komponen yang menaksir kontribusi produktifitas dari investasi.

Pada saat ini, pihak manajemen bisnis perusahaan sudah mulai mendapat gambaran. Survei menunjukkan bahwa rata-rata sekuritas mewakili sekitar 11% budget TI perusahaan pada Tahun 2003, sebuah kenaikan dibanding pada Tahun 2002 yaitu sekitar 9,5%. Pada saat ini perusahaan telah memberikan budget yang tersendiri untuk sekuritas supaya lebih memudahkan perhitungan pada budget TI, walaupun sebagian besar (78%) masih memasukkan sekuritas seba-

gai bagian dari keseluruhan budget TI.

Mendefinisikan pengembalian investasi sekuritas bukanlah sebuah tugas yang mudah, tapi setiap manajer TI bertanggung jawab untuk membuat perhitungan sendiri untuk menangani resiko yang akan dihadapi pada bisnis mereka. Perusahaan yang memandang pengembalian investasi keamanan secara sederhana sebagai masalah dari pembiayaan pribadi dan sumber daya TI akan tertinggal. Sekuritas harus dipertimbangkan sebagai sesuatu yang berbeda, sesuatu yang memiliki nilai amat berharga.

Regulasi, Pengembalian Dan Reputasi

Resiko yang harus ditanggung merupakan kekuatan dari pengembalian investasi pada investasi sekuritas. Masalah seputar memproteksi organisasi dari kerugian berhubungan dengan tiga faktor bisnis yaitu regulasi, pengembalian, dan reputasi (nama baik). Kepercayaan pelanggan adalah salah satu dari fokus perhatian pada sekuritas dan merupakan pembahasan penting pada diskusi untuk pembiayaan sekuritas. Sebuah survey yang dilakukan oleh Majalah CEO (Chief Executive Officer) pada Tahun 2002 menunjukkan bahwa pemerintah Amerika dan peraturan industri merupakan faktor pendorong terkuat pada pembelanjaan sekuritas (22%) diikuti oleh kebutuhan untuk mengurangi kerugian finansial (21%) dan penambahan kepuasan pelanggan (15%).

Dibanding dengan regulasi dan pengembalian, reputasi adalah masalah yang paling sulit dihitung, namun secara potensial adalah yang paling mahal. Reaksi masyarakat pada pencurian daftar pelanggan, mengidentifikasi angka-angka, informasi pasien atau data lain adalah pelanggaran sekuritas dan merupakan publisitas buruk yang dapat menghancurkan sebuah perusahaan. Manajemen TI haruslah dapat secara obyektif menaksir dan mengukur resiko sebuah pelanggaran sekuritas yang berakibat buruk pada reputasi organisasi.

Pertimbangan (Justifikasi) Pengembalian Pada Investasi Sekuritas

Investasi pada sekuritas dapat meredam berbagai ketakutan, ketidakpastian dan keraguan yang merupakan momok pada masa lalu. Pengembalian investasi sudah merupakan hal yang biasa pada industri saat ini, namun jaringan terbuka telah meruntuhkan semua model investasi sekuritas yang berbasis pengembalian investasi. Sifat terbuka dari jaringan pada saat ini membuat taksiran dari resiko (ancaman dan penyerangan) menjadi sulit untuk dihitung. Model pengembalian investasi keamanan memungkinkan petugas sekuritas untuk mempresentasikan sebuah analisis dari infrastruktur sekuritas suatu organisasi. Dengan demikian keuntungan bisnis yang dihasilkan dari usulan investasi pada sekuritas menjadi jelas. Pengembalian investasi keamanan menggabungkan pengurangan ongkos dihubungkan dengan meredakan resiko dan pertambahan produktifitas dihubungkan deangan investasi pada sekuritas. Tantangan

mendasar pengembalian investasi keamanan adalah untuk mengatasi masalah jaringan terbuka pada sekuritas tanpa menghapus keuntungan besar dari jaringan terbuka itu sendiri.

Pengembalian investasi adalah pengembalian pada modal yang diinvestasikan, sebuah pengukuran pada unjuk kerja perusahaan. Pengembalian investasi bersifat sudah tertentu karena total dari modal dibagikan pada pendapatan perusahaan, kadang-kadang sama dengan pengembalian pada aset. Pihak bisnis mendefinisikan pengembalian investasi sebagai sebuah penambahan bobot pada sebuah kegiatan. Terdapat tiga cara untuk menambah pengembalian investasi yaitu dengan meminimalkan ongkos, memaksimalkan pengembalian dan mempercepat waktu pengembalian.

Pengembalian pada investasi sekuritas didefinisikan sebagai harga yang harus ditanggung akibat kehilangan kepercayaan. Hal itu akan mereduksi jumlah investasi sekuritas. Pengembalian investasi keamanan adalah masalah yang belum dapat dipastikan, tidak tentu karena tidak memiliki batas yang pasti. Beberapa investasi pada sekuritas telah memiliki pengembalian investasi yang spesifik, seperti jumlah pengguna yang sudah pasti dan asuransi pada perusahaan. Pengembalian investasi keamanan juga didefinisikan sebagai penambahan bobot pada sebuah kegiatan.

Terdapat empat cara untuk menambah pengembalian investasi keamanan yaitu dengan meminimalkan atau menghapus kerugian operasional, meminimalkan investasi, memaksimalkan pengembalian positif dimana pengembalian investasi dipakai, mempercepat waktu pengembalian.

Dasar-dasar yang harus dipahami untuk menambah pengembalian investasi keamanan :

1. Sasaran objektif perusahaan untuk sekuritas adalah menghasilkan dokumen cetak biru pimpinan yang digunakan untuk memahami rencana 5 tahun ke depan mengenai kemajuan teknologi dalam perangkat keras, perangkat lunak dan jaringan
2. Caranya adalah dengan melakukan kontak dengan pihak yang dapat memenuhi kebutuhan legal dan kelompok industri untuk memahami waktu jangka pendek/panjang dan kebutuhan untuk waktu singkat
3. Menganalisis resiko yang dihadapi, mengerti resiko awal pada dunia *cyber*/ fisik sekuritas, pemulihan bencana/bisnis yang berkelanjutan dan pemenuhan untuk proteksi data/peraturan pada pembagian data.
4. Menghitung pengaruh yang mungkin untuk setiap insiden dan kerugian yang potensial. Kemungkinan kejadian yang sesuai dengan kenyataan, menggunakan persentasi untuk mempengaruhi pengubahan, menarik tren informasi industri, pemberian suara pada pemerintah/industri dan menghitung kerugian internal sebelumnya.
5. Pengaruh yang kuat pada kejadian nyata adalah dengan memperhitungkan pengaruh rupiah yang nilai-

nya tetap, menaksir nilai rupiah yang nilainya berubah berdasarkan kerugian pada pengeluaran industri, pemberian suara pada vendor industri

6. Keuntungan untuk perusahaan adalah penghindaran yang merupakan suatu keuntungan, tetapi dasar kebenarannya lemah untuk bisa memenangkan pemberian biaya, pengurangan kerugian – proyek kuda-kudaan, proyek yang disetujui haruslah memiliki keterkaitan dengan proyek berikutnya dan dapat membuat rencana yang komprehensif untuk menyerang bagian pendanaan.

Cara merencanakan justifikasi untuk sekuritas adalah :

1. Tiga wilayah primer untuk sekuritas adalah rencana DRP/ BCP, yaitu deteksi, reaksi dan pencegahan. Sekuritas harus mempunyai kemampuan mendeteksi berbagai percobaan yang dilakukan untuk menyalahkangunakan aset perusahaan; kemampuan dalam merespon kejadian haruslah ditentukan terlebih dahulu supaya efektif, sebuah titik pada waktu kejadian memboroskan waktu, uang dan sumber penghasilan dan menambah pembukaan, sekuritas harus dapat mencegah intrusi melewati cyber/ dinding fisik perusahaan.
2. Memprioritaskan untuk meredakan resiko – membangun sebuah gambaran resiko, membuat urutan resiko berdasarkan hal-hal berikut :
   - Kekritisan (peliknya pengaruh – operasional atau keuangan)
   - Biaya untuk meredakan resiko (biaya keseluruhan dari kepemilikan)
   - Jangka waktu proyek, gunakan kelipatan waktu per tiga bulan untuk dapat tambahan waktu dalam menyelesaikan proyek yang melebihi waktu
   - Tentukan sebuah nilai yang berhubungan untuk masing-masing resiko
3. Sumber-sumber yang dapat digunakan, yaitu : sejumlah staf khusus/para kontraktor/staf tambahan yang diperlukan untuk mencapai sukses; pelaksanaan proyek apa yang berjalan bersamaan dan menggunakan sumber-sumber yang sama/pemberian pembiayaan; pewaktuan, untuk menambah batas waktu internaldan eksternal; perputaran anggaran belanja yang ada atau yang harus direncanakan untuk fiskal pada tahun berikutnya atau untuk pemerintah.

Rencana komprehensif untuk meyakinkan manajemen dilakukan dengan :

1. Menggunakan gambaran resiko sebagai sumber dari penentuan proyek. Resiko dibagi secara bertingkat kedalam strategi dan taktis (titik kritis, tinggi, pertengahan dan pendek); memasukkan audit pada proses evaluasi untuk menentukan apa yang telah diidentifikasi sebelumnya, hasil audit biasanya dapat dipercaya; gambaran resiko dipresentasikan pada manajemen

yang sesuai untuk dipelajari, melakukan lobby agar resiko yang kredibel dapat diterima.

2. Merencanakan proyek yang dapat menjadi landasan bagi proyek lain dengan cara merencanakan proyek strategis yang berhubungan dengan taktis; mencari pendanaan untuk proyek DRP, membangun solusi/fondasi teknologi; sudah terdapat para pegawai atau sumber-sumber industri agar tercapai sukses sesuai waktu yang ditetapkan
3. Cara membuktikan bahwa suatu proyek akan berhasil dan menguntungkan perusahaan :
   - Sukses pada awal pelaksanaan proyek – dengan menggunakan manajer proyek yang berkualitas – menghindari memulai dengan apa yg tidak dapat diselesaikan sesuai dengan pepatah sama-sama menang (win-win solution).
   - Kebanyakan sekuritas dibiayai dengan kapitalisasi sehingga haruslah diketahui kebutuhan finansialnya.

Cara membangun sebuah kasus bisnis :

1. Memahami biaya total kepemilikan. Biaya total kepemilikan menggunakan keuangan untuk membantu rencana 5 tahun fiskal berikutnya (mengerti dimana harus dilakukan pemotongan bila diperlukan), kenyataannya kebanyakan pengeluaran investasi adalah OMAG sesudah tahun pertama (kapitalisasi pada tempat yang memungkinkan)
2. Batas waktu dan sumber-sumber yang diperlukan. Memfokuskan pembicaraan pada keadaan saling ketergantungan antara para pemrakarsa keamanan. Membicarakan rencana yang besar-besar; pemanfaatan silang sumber daya. Menggunakan batas waktu federal/pemenuhan syarat-syarat untuk kemajuan. Melakukan kontak dengan perusahaan industri sedini mungkin untuk menentukan sumber-sumber yang dapat digunakan. Meminimalkan pengeluaran (pembiayaan)/ menyimpan untuk perbekalan di masa datang.
3. Menggunakan pengukuran finansial dengan cara membangun ukuran yang dapat merefleksikan kemajuan proyek, tanggapan kejadian, deteksi interusi, biaya untuk menghindar; selalu siap menaksir biaya finansial untuk menghindar dari suatu kejadian; menyediakan umpan balik jangka pendek yang harus dicapai dan bukti yang mendukung penggunaan pengembalian investasi keamanan di masa yang akan datang
4. Pekerjaan finansial yaitu melakukan kapitalisasi segala tempat yang memungkinkan; kapitalisasi, penggunaan uang direfleksikan secara berbeda pada pencatatan; berhati-hati dalam memahami dan mengkategorikan masalah permodalan.
5. Menekankan pada pengaruh dengan cara: menekankan pada pelindung apa yang dapat berfungsi

untuk mencapai keuntungan yang diharapkan, apa saja pengaruh yang spesifik dan keuntungan yang spesifik dari masing-masing proyek; *Piggyback* menghubungkan proyek untuk menyediakan tambahan nilai keuntungan sesuai dengan standar pengembalian investasi keamanan

6. Mencari tahu kebutuhan sekuritas para pemegang keputusan dengan cara menuliskan narasi berisi harapan untuk para pemegang keputusan proyek dan mencari tahu kebutuhan sekuritas yang diperlukan untuk menyelesaikan pekerjaan pada bidang masing - masing (keuangan, keorganisasian, manajemen sumber daya, struktur, bonus, dan lain-lain).

Perhatian dari pihak yang berkepentingan harus didapatkan. Dalam hal ini pembicaraan haruslah menekankan pada resiko dan pengaruh yang kuat. Personil sekuritas harus dapat menemukan sumber uang, kemudian membawanya kepada para ahli resiko untuk dievaluasi. Setelah itu membuat alternatif untuk meredakan resiko dari berbagai sisi dan membuat rencana yang sesuai dengan rencana perusahaan.

Langkah selanjutnya adalah memberikan pengertian mengenai semua kemungkinan yang dapat diterima, memberikan alternatif mengenai cara menghindari dan cara meredakan resiko. Untuk itu informasi yang kontinu pada pihak yang berkepentingan mengenai kerangka kerja sekuritas yang komprehensif (DRP/BCP) dan membuat laporan mengenai cara mengukur secara reguler adalah penting. Bila sasaran telah diketahui, maka kebutuhan yang diperlukan akan dapat diupayakan.

Kesuksesan dapat didasarkan pada keadaan keseimbangan antar pengembalian yang dapat dihitung dengan pengurangan resiko dan kemajuan yang diharapkan dari perspektif bisnis. Lebih penting lagi, orang sekuritas haruslah dapat menangkap keuntungan yang sebenarnya dan nilai dari proyek yang ada pada kondisi yang sedang berjalan. Hal ini dapat membantu kredibilitas dan meyakinkan para pengambil keputusan untuk melicinkan proses perijinan bagi proyek baru.

Proses dalam menjadikan proyek sekuritas menjadi sesuatu mempunyai dasar yang kuat telah matang dan akan dipengaruhi pula oleh kematangan dari proses dalam menaksir resiko sehingga akan menambah pemahaman eksekutif mengenai aturan main dalam kerangka bisnis. Pada masa mendatang, manajer sekuritas yang sukses akan mengerti bisnis dengan lebih baik lagi dan manajer bisnis akan lebih mengerti landasan dari pengembalian investasi keamanan.

Evaluasi Biaya Dan Keuntungan Pada Sekuritas

Pengembalian investasi telah merupakan sebuah topik yang besar bagi kepentingan manajemen untuk infrastruktur TI. Pengembalian investasi untuk sekuritas atau pengembalian investasi keamanan telah mendapat perhatian khusus, mungkin karena sekuritas adalah sebuah tradisi seperti

sebuah bidang yang tidak dapat diduga. Pengembalian investasi keamanan masuk ke dalam aliran penting dari pemikiran manajemen TI pada awal Tahun 2002 dengan sebuah artikel dari majalah CEO (Chief Executive Officer). Beberapa artikel non teknis lain muncul pada saat itu menawarkan saran bermutu dan metode secara garis besar. Majalah Computer World kemudian membuat sebuah "pusat pengetahuan" untuk topik pengembalian investasi. Walaupun hanya sedikit dari isi yang ada berhubungan dengan informasi sekuritas, situs web tersebut berisi sebuah materi tutorial yang bagus, keterhubungan pada alat yang bermutu dan potongan pendapat yang berguna untuk masalah yang berhubungan dengan estimasi pada pengembalian investasi.

Terdapat beberapa cara untuk mengevaluasi biaya-keuntungan investasi pada sekuritas yang banyak digunakan pada 10 tahun belakangan ini, diantaranya adalah justifikasi kualitas untuk investasi sekuritas, harapan kerugian per tahun, metode evaluasi atribut sekuritas, analisis efektifitas biaya, analisis pohon kesalahan, pembatasan pendekatan yang ada dan lain-lain.

Justifikasi tradisional untuk pengeluaran sekuritas kebanyakan secara mutu atau strategi, dengan pendapat itu, tanpa investasi, organisasi akan kehilangan keuntungan yang besar.

Beberapa poin pada pengeluaran untuk sekuritas meliputi sekuritas mewakili ongkos dalam melakukan bisnis; sekuritas merupakan jenis dari ongkos asuransi; aliran pengembalian melalui e-bisnis tergantung pada sekuritas yang tepat; sekuritas adalah salah satu aspek dari manajemen resiko; aksi legal dapat dihasilkan dari kegagalan sebuah tugas sesuai dengan standar sekuritas minimum; ketidaksetujuan dengan pengeluaran sekuritas pada saat sekarang dapat menyusut seiring usia kematangan informasi; pada suatu ketika, tidak ada lagi yang menanyakan harga dari bangunan sekuritas.

Secara kuantitas, kasus bisnis yang secara finansial kuat sangat memerlukan investasi pada sekuritas. Para pihak yang berkepentingan, seperti keuangan, tidak akan goyang oleh pendapat tentang mutu saja.

Model pengembalian investasi keamanan yang diberitakan pada majalah CEO (Chief Executive Officer) bulan Februari 2002 dirumuskan di universitas IDAHO dan institusi lain sebagai ekspektasi kerugian per tahun. Dasar pendekatannya adalah dengan menghitung kerugian yang harus dihadapi oleh sebuah organisasi dan membandingkan kerugian tersebut dengan investasi sekuritas yang diperlukan untuk meredakannya.

Perkiraan kerugian tahunan berasal dari cabang informasi sekuritas yang dicobakan secara empiris dari pengalaman organisasi dan cerdas dalam hal gangguan (intrusi), virus, serangan penolakan layanan dan lain-lain. Kerugian dapat dianggap, setidaknya untuk sektor organisasi privat, sebagai berikut:

1. Kehilangan pengembalian dari situs e-commerce akan merugikan waktu;

2. Kehilangan kepercayaan dari klien akan berakibat merugikan;
3. Lembur yang dibayarkan pada staf TI dan kontraktor tambahan berguna untuk mengembalikan sistem pada jalurnya;
4. Biaya untuk konsultasi dengan para spesialis dari luar mengenai pemulihan data, perbaikan, forensik, pekerjaan legal dan sebagainya;
5. Kerusakan akibat kejahatan *cyber* atau pelanggaran privasi;
6. Tagihan reparasi untuk kerusakan fisik yang dihasilkan dari serangan *cyber* pada sektor tertentu seperti air dan penggunaannya.

Untuk mengurangi kerugian yang diperkirakan, organisasi haruslah menginvestasikan sejumlah uang pada bidang sekuritas, termasuk benteng untuk membatasi para penyerang mendapatkan akses, sistem deteksi intrusi (gangguan untuk) peringatan awal dengan pengintaian yang mendahului kelompok penyerangan, dan pengukuran anti virus untuk mendeteksi kode jahat dalam bentuk yang berbeda-beda.

Bila organisasi menetapkan untuk membuat dan mengoperasikan sistem sekuritas, maka biaya yang harus ditanggung terdiri dari :

1. Ongkos persiapan, meliputi harga lisensi produk sekuritas, server dan perangkat keras lain, dan ongkos konsultasi untuk menganalisis dan membuat konfigurasi;
2. Ongkos perawatan, meliputi dukungan produk sekuritas dan biaya pemeliharaan, gaji staff TI sekuritas dan biaya menghidupkan sistem, biaya sewa asosiasi dan tambahan staf sekuritas, dan biaya penelitian untuk perkiraan ancaman yang sedang berlangsung dan evaluasi secara berkala pada teknologi baru.

Sasaran pengembalian investasi keamanan adalah untuk meminimalkan atau bahkan menghilangkan kerugian operasional, meminimalkan investasi, memaksimalkan keuntungan dan mempercepat waktu pengembalian. Sangatlah sulit tapi masih memungkinkan untuk mendapat sebuah kesepakatan di antara para praktisi sekuritas dalam menetapkan pengembalian investasi keamanan untuk sebuah perusahaan. Perhitungan pengembalian investasi keamanan yang cukup efektif bagi para praktisi adalah menggunakan pendekatan dari atas ke bawah.

Menggunakan pendekatan ini, sebuah badan milik pemerintah Amerika merumuskan sebuah strategi sekuritas yang dapat dieksekusi menggunakan sebuah peta jalur pragmatis antar perusahaan. Jalur peta disebarkan melintasi beberapa tingkatan perusahaan dan dilakukan berulang-ulang sehingga menjadi pelajaran yang dapat dikuasai selama siklus kehidupan. Arah dari jalur peta harus selalu diluruskan dengan mencocokkan atau melakukan modifikasi berdasarkan ketergantungan pada inisiatif taktis secara terus menerus.

Tujuan utama dari pendekatan ini adalah untuk :

1. Mendefinisi secara lengkap syarat untuk seluruh perusahaan dan/atau program

atau portofolio atau proyek yang terlibat di dalam perusahaan.

2. Menetapkan sasaran bisnis yang harus dicapai oleh masing-masing unit bisnis atau sebuah perusahaan secara keseluruhan, terutama difokuskan pada pengaruh kritis sekuritas sebagai sebuah pembiayaan.
3. Menaksir jumlah manajemen dan bisnis pemakai yang menyadari kelemahan, mudah diserang, ketersediaan dan ketanggunhan sistem.
4. Menganalisis teknologi dan operasi yang efisien pada terminologi nilai keuntungan dan keefektifan sehingga sesuai dengan tujuan sekuritas.

Secara umum, perusahaan dengan perhitungan sekuritas yang kuat menggunakan sebuah rumus, yang dikembangkan oleh para periset dari Universitas IDAHO untuk mendefinisikan pengembalian investasi keamanan, seperti yang ditunjukkan persamaan (1).

Rumusnya adalah :

ROSI = R – ALE (1)

ALE = (R - E) + T (2)

ALE (*Annual Loss Expectancy*) = kerugian tahunan.

R = biaya tahunan untuk penggantian angka intrusi (gangguan).

E = dollar yang berhasil dihemat dengan menggunakan perangkat.

T = harga dari perangkat pendeteksi intrusi.

Pengembalian investasi keamanan harus lebih besar dari atau sama dengan perbedaan dari R dan ALE. Saran ini didasarkan pada fakta bahwa pada banyak kasus perusahaan kecil gagal menjadi perusahaan besar yang memiliki tingkat pengukuran sekuritas karena kerumitan dari implementasi dan ketekunan yang wajib untuk memperoleh kerjasama dari manajemen senior. Secara khusus, sebuah instalasi yang pantas dan sistem pertahanan lingkungan dapat menerima sekitar 85% keefektifan dalam pencegahan atau meredakan pelanggaran sekuritas. Keadaan itu dapat dipertahankan sepanjang instalasi tersebut dipelihara dengan baik dan secara berkala diperbaiki sesuai dengan kebutuhan.

Keuntungan keuangan bersih dari sebuah lingkungan sistem sekuritas pada model ALE adalah sebagai berikut:

$$\text{Simpanan Tahunan} = \text{ALE} \times \text{Efektivitas} - \text{By. Tahunan} \quad (3)$$

Di dalam model ALE diasumsikan bahwa seluruh pelanggaran sekuritas membawa biaya yang sama untuk implikasinya, jadi bila kita menghemat 85% pelanggaran, maka akan diasumsikan penghematan biaya sebanyak 85% .

Menurut observasi, ada beberapa hal yang penting untuk dilakukan:

1. Menggunakan sebuah kesepakatan dengan pendekatan tertentu yang mengikuti aturan pengukuran sekuritas dan mandat dari pemerintah atau regularisasi.
2. Mengukur kebutuhan pemakai dan kejadian sekuritas seperti pelanggaran atau gangguan (intrusi) pada terminologi penghematan biaya secara keseluruhan dari perusahaan.

3. Melakukan audit secara periodik untuk menggambarkan perubahan yang terjadi atau modifikasi yang harus dibuat untuk menghitung sekuritas yang memadai untuk digunakan, dan juga untuk menilai keefektifan dari sekuritas yang dipakai pada saat ini.

Sangatlah penting untuk mengumpulkan informasi yang relevan seperti sistem pengukuran untuk menentukan pengembalian investasi keamanan. Sangat dianjurkan bagi para praktisi untuk mengembangkan nilai yang dapat dimengerti dan hasil dari pengembalian investasi keamanan, sehingga pengembalian investasi sesungguhnya untuk sekuritas pada sebuah perusahaan dapat dicapai. Dari pandangan bisnis pengembalian investasi keamanan harus berhubungan dengan nilai yang terintegrasi dari sebuah perusahaan seperti efesiensi organisasi, integritas data dan jumlah penghematan, sementara itu penerimaan hasil juga sesuai atau melebihi perkiraan yang diharapkan oleh pelanggan, sejalan dengan batasan yang mendukung persaingan.

Metode evaluasi perlengkapan sekuritas telah dikembangkan pada universitas Carnegie Mellon untuk memproduksi keuntungan yang mapan. Dibandingkan dengan arsitektur sekuritas lainnya, dalam bahasa nyatanya adalah bahwa para ahli sekuritas jarang memiliki data keuntungan yang akurat dalam bidang teknologi.

Kebanyakan ahli sekuritas memiliki pemahaman yang kurang dibanding para manajer pemrograman, kadang mereka hanya memiliki pengalaman, intuisi dan pendapat sendiri. Intuisi dapat memiliki kekuatan namun dapat pula membuat kesulitan untuk manajer yang bukan ahli untuk secara obyektif m*ereview* rekomendasi pada sekuritas. Metode evaluasi atribut sekuritas menggabungkan kemungkinan tinjauan mendalam dan kedudukan pengaruh yang lebih kuat untuk bagian dari lingkungan yang ditanyakan, dan mengirimkan biaya yang bervariasi yang saling berhubungan dan keuntungan dari alternatif desain sekuritas. Metode evaluasi atribut sekuritas tidak mengirimkan kuantitas estimasi biaya yang berdiri sendiri.

Di negara Australia, analisis efektifitas biaya pada akhir-akhir ini lebih diaplikasikan pada sektor kesehatan, untuk dipelajari kemajuan performasinya sebagai hasil dari investasi yang diusulkan pada sistem yang baru. Satu kekuatan dari analisis efektifitas biaya adalah mengakomodasi pengukuran performasi non-financial; sebagai contoh pada praktek klinis, dapat mengembalikan persentase kemajuan mortalitas yang mengintervensi satu jenis perawatan kesehatan melebihi jenis yang lainnya.

Teknik digunakan untuk membandingkan kandidat alat pengukur sekuritas, penaksiran yang tergantung dari keragaman pengukuran performansi, seperti pada ketersediaan sistem.

Sebuah pohon kesalahan adalah sebuah alat grafis yang melakukan pencatatan semua mode kesalahan dari sebuah sistem yang rumit menjadi kombinasi logika, hubungan sederhana gerbang AND dan OR. Kesalahan yang dimaksud

di sini adalah kesalahan komponen. Data yang baik dapat dipakai sebagai dasar kesalahan dari seluruh komponen kritis, sedangkan analisis pohon kesalahan dapat membangkitkan kesalahan dasar yang telah diduga sebelumnya pada keseluruhan sistem.

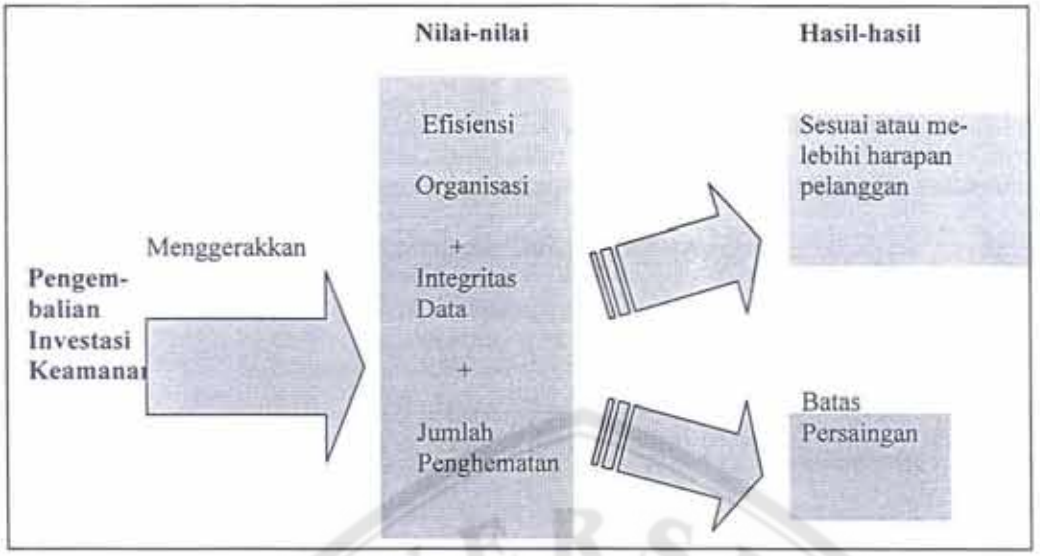
Teknik pohon kesalahan pada sekuritas TI digunakan dengan cara membuat sebuah pohon yang menggambarkan hubungan sebab akibat antara vektor penyerang dengan kesalahan sistem. Aplikasi dari tindak balas diharapkan akan memangkas cabang dari pohon kesalahan sehingga seluruh akibat dapat dibandingkan. Analis pohon kesalahan didasarkan pada asumsi kembar, kegagalan komponen secara acak sesuai dengan hasil statistik dan pada level terendah pohon kesalahan, kesalahan komponen tidak tergantung dengan yang lainnya. Pada perangkat lunak TI, kesalahan tidaklah acak, tetapi lebih pada desain kesalahan yang sistematis. Pada kebanyakan perangkat lunak, kesalahan pada kode online dapat berakibat pada bagian lain dari program sehingga penggunaan pohon kesalahan dan keahlian teknis akan dapat membantu.

Terdapat beberapa pembatasan dari pendekatan yang telah disebutkan di atas. Kelemahan utama dari seluruh analisis di atas adalah belum ada tindak balas yaitu dapat memberikan sejumlah harga atau keuntungan dari sekuritas yang dipakai secara individual. Metode evaluasi atribut sekuritas dan analisis efektifitas biaya berfungsi untuk memprioritaskan keuntungan sesuai dengan tindak balas yang dipilih, namun mereka tidak menyediakan garis dasar dari data keuangan. Saat ini yang paling dikenal adalah sebuah pendekatan kuantitatif. Perhitungan dengan harapan kerugian per tahun menggulung kontribusi dari semua tindak balas menjadi sebuah gambaran tunggal keefektifan.

Sampai saat ini belum ditemukan metode untuk menghitung gulungan keefektifan. Model ALE juga cacat dengan asumsi bahwa semua pelanggaran sekuritas memiliki biaya yang sama. Bila biaya tahunan untuk kesalahan pada sekuritas $10 juta, dan sistem tersebut memiliki efektifitas 85%, hal itu bukan berarti bahwa sistem tersebut dapat menghemat $8,5 juta. Bila kejadian dari pelanggaran yang beresiko mahal sekitar 15%, maka kita dapat menggunakan pendekatan ALE.

Masih ada suatu model pengembalian investasi keamanan lain yang dinamakan *Hybrid* pengembalian investasi keamanan, merupakan hasil dari NSW *Departement of Commerce Office of Information and Communications Technology* (OICT) milik pemerintah Australia, yang memadukan ALE dengan *Australian-standard Threat and Risk Assessment* (TRA). Model ini direkomendasikan dengan 4 alasan, yaitu:

1. Model ini menggunakan pendekatan finansial kuantitatif;
2. Model memberikan tindak balas sekuritas yang berbeda sesuai kontribusi yang diberikan pada seluruh biaya-keuntungan;
3. Model ini membuat penggunaan alat sekuritas meluas dan lebih dikenal se-



Gambar 1. Sistem Pengukuran Untuk Menentukan Pengembalian Investasi Keamanan

Gambar 2. Tipe Tindak Balas

hingga mudah dipakai dengan sedikit pelatihan;

4. Model ini bisa diperluas seperti membuat biaya sekuritas menggunakan model statistik tersebar dengan variabel natural dan pengaruh dari ancaman nyata pada sekuritas.

Pada *Hybrid* pengembalian investasi keamanan, sebuah tindak balas sekuritas dapat memiliki satu atau 2 buah efek ancaman. Pertama, mengurangi kemungkinan munculnya ancaman sebagai sebuah peristiwa. Kedua, mengurangi beratnya musibah yang seharusnya terjadi.

Tindak balas dapat dikatakan sebagai tindakan pencegahan bila dapat mengurangi kemungkinan ancaman dan disebut kuratif bila dapat mengurangi beratnya akibat yang ditimbulkan dari penyerangan. Istilah itu tentu saja bisa saling tumpang tindih seperti terlihat pada Gambar 2.

Seperti terlihat pada Gambar 2, efek dari tindak balas cenderung kepada preventif yaitu mencegah kejadian, daripada kuratif atau mengurangi akibat dari suatu kejadian sekuritas. Tabel 1 berikut berisi contoh untuk masing-masing tipe tindak balas.

Tabel 1. Contoh-contoh Tindak Balas

Tipe Tindak Balas	Contoh
Preventif	Standarisasi, Prosedur-prosedur dan garis pedoman, Audit-audit, Inspeksi, Latihan-latihan, Firewall, Deteksi intrusi virus dengan Content Scanning, Enkripsi, Mengklasifikasikan data
Kuratif	Sistem-sistem yang redundant, Backup
Keduanya	BCP/ DRP, Training

PENUTUP

1. Investasi pada sekuritas sulit untuk dihitung walaupun kebutuhan akan sekuritas sudah diketahui dan pengaruhnya nyata namun dasar pembenarannya sebelum waktu kejadian adalah sulit. Langkah-langkah bisnis dapat digunakan untuk mendefinisikan sebuah perhitungan yang realistis untuk menentukan pengaruh dari kepercayaan untuk investasi pada sekuritas yang tepat.
2. Investasi pada sekuritas adalah sebuah proses yang kompleks dan dinamis. Metodologi baru untuk menghitung pengembalian investasi pada teknologi keamanan menawarkan sebuah kemajuan penting dalam mempercepat proses. Disamping itu juga memberikan data pokok yang sifatnya tidak dapat dipercaya. Tidak ada perusahaan yang akan berjalan sendirian pada era teknologi jaringan terbuka. Sebuah taksiran yang teliti dari resiko harus menjadi garis landasan yang mewataki keputusan yang dibuat pada investasi keamanan.
3. Investasi pada sekuritas harus mempertimbangkan penggerak bisnis bukan penghalang bisnis. Menyuguhkan nilai sekuritas adalah suatu masalah asuransi dari teknologi yang dapat menggerakkan bisnis elek-

tronik. Kebijaksanaan sekuritas dan prosedur dihubungkan langsung dengan sasaran bisnis dan mengatur serta memelihara teknologi sekuritas semaksimal mungkin dari nilai investasi yang dibayarkan. Analisis pengembalian investasi keamanan dapat diterapkan untuk menghitung tingkat pengembalian dari penanaman modal pada sekuritas. Dengan demikian tantangan mendasar pengembalian investasi keamanan untuk mengatasi masalah jaringan terbuka pada sekuritas tanpa menghapus keuntungan-keuntungan besar dari jaringan terbuka itu sendiri akan tercapai.

DAFTAR PUSTAKA

A Guide to Security Risk Management for Information Technology Systems. Published by the Government of Canada Communications Security Establishment. 1996. Http: www.cse.dnd.ca/en/documents/knowledge_centre/publications/manuals/mg2e.pdf

Achieving Appropriate Return on Your Security Investment Effectively. Locheed Martin information Technology. http: www.lmco.com/locheed/martin/pengembalian investasi keamanan.pdf.

Budi Rahardjo. **Keamanan sistem informasi berbasis internet.** PT. Insan Indonesia – Bandung dan PT. INDOCISC. Jakarta. 2002.

Budi Rahardjo. **Panduan Menulis dan Mempresentasikan Karya Ilmiah : Thesis, tugas akhir dan makalah**. 4 Januari 2004. http :www.budi.insan.co.id/books/thesis/

Calculated Risk Scott Berinato in CSO Magazine. December 2002. http: www.csoonline.com/read/120902/calculate.html.

Computer Crime and Security Survey. FBI/CSI 2003. Computer Security Institute. 2003

Computer World ROI Knowledge Centre at www.computerworld.com/ managementtopics/roi.

Corsaire - Articles – Evaluating the return on security investment (ROSI) Where's the problem. 7 July 2003. http: www.corsaire.com/articles/2003/07/02_02.htm.

Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending Timothy Braithwaite in Information Systems Security. Auerbach Publications. September/ October 2001.

Finally, a Real Return on Security Spending CIO Magazine. 15 February 2002. http: www.cio.com/archive/021502/security.html.

Information Security Guideline Part 1 - Risk Management NSW Government Office of Information and Communications Technology. June 2003. http: www.oict.nsw.gov.au/content/2.3.16-Security-Pt1.asp.

Information Security Risk Management Guidelines SAA HB 231:2000.

Published by Standards Australia. 2000.

Justify the Return on Security Investment. L Chris N Shepherd. Nebraska CERT. 2003. http: www.icctcorp.com/~balepin /new pubs/costbenefit.pdf.

Primer on Cost-Effectiveness Analysis. Published by the American College of Physicians' Effective Clinical Practice. September/October 2000. See www.acponline.org/journals /ecp/sepoct00/primer.htm.

Return on Invesment for Information Security. Http: //www.oit.nsw.gov.au/7.1.1 5.ROSI.asp tanggal 3/2/ 2005

Return on Security Investment (ROSI). CIO. 15 February 2002. http: www.csoonline.com/glossa ry/index.cfm.

Risk Management Handbook 3. Australian Communications - Electronic Security Instruction 33 V1.0 (ACSI 33). Published by Defence Signals Directorate. 2000.

Secure Business Quarterly. **Special Issue on Return on Security Investment**. Quarter 4. 2001. See www.sbq.com/sbq/pengem balian investasi keamanan/ index.html.

Security Attribute Evaluation Method: A Cost-Benefit Approach Shawn A. Butler. Computer Science Department. Carnegie Mellon University. 2002. http: www2.cs.cmu.edu/~Compo se/ftp/SAEM-(Butler)- ICSE 2002.pdf .

Security Metrics Guide for Information Technology Systems Special Publication 800-55 US National Institute of Standards and Technology Computer Security Research Centre. 2002. See csrc.nist.gov/ publications/nistpubs/800- 55/sp800-55.pdf.

Steve Foster. Bob Paci. **Analysis of Pengembalian investasi for Information Security, A White Paper**. http : www.getronics.com/

The State of Information Security. L. Cosgrove Ware, Worldwide Study conducted by CIO Magazine and PricewaterhouseCoopers. 2003.