KAJIAN BISNIS DAN EKONOMIS DALAM MENGIMPLEMENTASIKAN *INFORMATION SECURITY* DI PERUSAHAAN

Oleh : Amru Yasir

Abstrak

Penelitian ini bertujuan untuk mengetahui kajian bisnis dan ekonomis dalam mengimplementasikan information security di perusahaan. Penelitian ini mengguankan metode penelitian pustaka (library research). Penelitian ini dilakukan dengan mengkaji kondisi lingkungan keamanan sistem informasi dalam sudut pandang ekonomi. Terjadi perubahan mendasar dalam menjalankan organisasi dari kegiatan tradisional ke organisasi yang terhubung dengan internet (e-business), sehingga asset perusahaan yang berupa informasi harus tetap terjaga dan terpelihara terhadap segala perubahan tersebut. Pemeliharaan informasi tak terbatas terhadap gangguan yang dilakukan dari pihak luar, tetapi juga harus mempertimbangkan gangguan yang dilakukan oleh pegawai perusahaan dan pengendalian arus data di dalam jaringan perusahaan. Pengamanan terhadap gangguan keamanan sistem informasi harus secara proaktif dilakukan baik oleh CISO maupun kebijakan perusahaan, jika tidak mau kehilangan kapitalisasi pasar akibat pemberitaan publik.

Kata kunci : *bisnis, ekonomis dan information security*

1. Pendahuluan

1.1. Latar Belakang

Suatu perusahaan atau organisasi memiliki sumber daya yang bersifat *tangible* maupun *intangible*. Untuk mendapatkan sumber daya tersebut, proses pengambilan keputusan akan dipengaruhi oleh hasil membandingkan antara biaya dan manfaat yang timbul dari akuisisi sumber daya tersebut. Hal ini tidak

terkecuali dalam aktifitas yang berkaitan dengan *information security*.

Model-model ekonomi tradisional untuk mengkaji tingkat pengembalian investasi atas pengeluaran perusahaan (*expenditures*) dibidang *information security* masih menjadi bahan perdebatan, mengingat aspek teknis dari *information security* (misal: teknik enkripsi dan *intrusion detection system*) sangat terbatas untuk dapat diterjemahkan kedalam aspek finansial.

Model *Net Present Value* (NPV) banyak dipergunakan untuk mengevaluasi sumber daya yang tangible sehingga manfaat dan biaya dapat diukur secara nyata. Jika model NPV tersebut dipergunakan maka perubahan manfaat (*incremental benefits*) yang terus menerus dari implementasi information security harus terukur. Sedangkan komponen terukur di bidang *information security* baru sebatas total biaya pengeluaran untuk pembelian aset fisik dari *information security*.

1.2. Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui kajian bisnis dan ekonomis dalam mengimplementasikan *information security* di perusahaan.

1.3. Metode Penelitian

Penelitian ini mengguankan metode penelitian pustaka (*library research*). Penelitian ini dilakukan dengan mengkaji kondisi lingkungan keamanan sistem informasi dalam sudut pandang ekonomi. Selanjutnya, dilakukan identifikasi model-model ekonomi tradisional dan moderen yang telah banyak dilakukan, sehingga keunggulan dari masing-masing model tersebut dapat dipergunakan. Hal tersebut tidak terlepas dari kondisi masing-masing organisasi.

2. Uraian Teoritis

2.1. Aspek-Aspek Ekonomi dari Keamanan Sistem Informasi

Dari survey yang dilakukan oleh *PriceWaterHouse-Coopers* pada tahun 2002 menunjukkan bahwa lingkungan bisnis yang terjadi di Inggris dan US telah terjadi perubahan, yakni dengan memberdayakan kemampuan internet untuk melakukan aktifitas *e-business*. Pemanfaatan internet ini memberi dampak langsung terhadap keamanan sistem informasi dan menjadikan internet sebagai pintu gerbang serangan ke sistem informasi suatu organisasi.

Dapat diketahui pula bahwa 69% total perusahaan dan 92% perusahaan besar yang disurvey memberikan kesempatan kepada pegawainya untuk mempergunakan akses *web*. Yang menarik dari hasil tersebut menunjukkan pula, hanya 13% perusahaan yang menerima transaksi perdagangan dengan menggunakan *customer online*.

Adapun aspek-aspek ekonomi dari *information security* yang menjadi pokok bahasan meliputi : (i): Seberapa sering/ frekuensi pelanggaran atas keamanan sistem informasi terjadi, (ii): Kerugian atas pelanggaran-pelanggaran keamanan sistem informasi, (iii): Proses investasi yang berkaitan dengan keamanan sistem informasi, dan (iv) Reaksi portfolio investor terhadap pelanggaran keamanan sistem informasi yang diumumkan untuk publik.

2.2. Frekuensi Pelanggaran Keamanan Sistem Informasi

Keberadaan internet telah menimbulkan resiko-resiko baru dalam menjalankan aktifitas *e-business*. Survey terhadap lebih dari 1400 organisasi yang dilakukan pada tahun 2003 di seluruh dunia oleh *Ernst & Young*, mengindikasikan bahwa intensitas ancaman keamanan sistem informasi paling tinggi dalam 12 bulan kedepan diakibatkan oleh *virus*. *Virus* mempunyai intensitas ancaman keamanan sistem informasi yang paling tinggi. Sedangkan intensitas ancaman urutan kedua diakibatkan oleh status

kepegawaian seseorang, dan diikuti dengan intensitas urutan ketiga yakni *distributed Denial of Servicess attack (DDoS)*.

Hasil temuan tersebut di atas sangat konsisten dengan survey yang dilakukan di Inggris tahun 2002 dan di USA 2003, dimana virus dan pegawai perusahaan mendominasi semua pelanggaran keamanan sistem. Untuk ancaman yang dihadapi oleh semua skala industri di Inggris menunjukkan bahwa infeksi virus merupakan ancaman terbesar (33%) dan diikuti dengan ancaman yang ditimbulkan oleh akses *illegal* untuk informasi rahasia dan sistem komputer (26%). Sedangkan kegagalan sistem menempati urutan ketiga (15%) dan urutan keempat merupakan serangan yang dilakukan *hacker* di *website* (11%).

Jika dibandingkan dengan hasil survey di Inggris di tahun 2002, 2000 dan tahun 1998, pelanggaran keamanan sistem informasi terjadi peningkatan yang sangat berarti. Sebagai contohnya, di tahun 1998 pelanggaran telah dialami oleh 18% responden. Selanjutnya terjadi peningkatan lebih dari dua kali di tahun 2002 yakni 44% untuk semua skala industri, sedangkan skala industri besar telah dialami oleh 78% responden.

2.3. Kerugian atas Pelanggaran Keamanan Sistem Informasi

Di Inggris, hampir dua pertiga kejadian pelanggaran menimbulkan kerugian kurang dari USD 15.000. Kerugian tersebut meliputi hilangnya kesempatan pendapatan biaya perbaikan, pegawai dan biaya lain yang berkaitan dengan pelanggaran tersebut. Hanya empat persen (4%) organisasi mengalami kerugian lebih dari US$ 750.000 untuk satu kali kejadian pelanggaran keamanan sistem informasi.

Di tahun 2003, CSI/FBI melaporkan bahwa 75 persen dari 530 responden mengalami kerugian atas pelanggaran keamanan sistem informasi, dan hanya 47% dari responden tersebut yang dapat menghitung kerugian tersebut[2]. Seperti diperlihatkan pada gambar 5, *total annual losses* terbesar diakibatkan oleh pecurian

informasi penting perusahaan yang mencapai US$ 70.2 juta. Kerugian tersebut telah mengalami penurunan lebih dari separuh kerugian, jika dibandingkan kerugian yang diakibatkan oleh dengan kejadian sama di tahun 2002 dan 2001, yakni US$ 171 juta dan US$ 151 juta.

Sedangkan total kerugian tahunan yang diakibatkan oleh *denial of services* sebesar US$ 66 juta. Kerugian di tahun 2003 mengalami peningkatan lebih dari tiga kali dibandingkan dengan kejadian sama di tahun 2002, dan mengalami peningkatan lebih dari 14x jika dibandingkan di tahun 2001.

Gangguan keamanan sistem yang diakibatkan oleh infeksi virus hanya menempati urutan ketiga dari total kerugian tahunan yakni sebesar US$ 27 Juta. Nilai kerugian tersebut tidak sebanding dengan intensitas ancaman yang diprediksi di 12 bulan kedepan yang menduduki prioritas tertinggi.

Dari kerugian keuangan yang diakibatkan dari beberapa jenis gangguan keamanan sistem informasi tersebut diatas, tercatat bahwa kurang dari sepertiga (33%) organisasi menutup kerugian keuangan tersebut dengan kebijakan perusahan masing-masing. Sedangkan 34% organisasi tidak menggunakan jasa asuransi untuk mengatasinya. Sisanya (33%) masih tetap menjadi persoalan di dalam organisaninya untuk mempertimbangkan penggunaan jasa asuransi dalam menutup kerugiannya.

Sampai saat ini masih menjadi suatu kendala dalam mengukur tingkat kerugian suatu perusahaan untuk memperoleh perlindungan dari jasa asuransi dalam menghadapi gangguan sistem kemanan tersebut. Keterbatasan tersebut tidak hanya dihadapi oleh pengelola perusahaan saja, tetapi juga oleh penyedia jasa asuransi.

2.4. Proses Investasi Keamanan Sistem Informasi

Biaya yang dikeluarkan untuk membangun keamanan sistem informasi sampai saat ini masih dianggap sebagai pengeluaran rutin (*expenses*) sehingga pengeluaran biaya tersebut tidak menjadi prioritas utama dan tidak diperlakukan sebagai investasi.

Konsekuensinya, keperluan untuk pengembangan keamanan sistem menjadi kendala karena keterbatasan anggaran biaya. Hal itu ditunjukkan dari hasil survey global dimana 56% responden menghadapi keterbatasan anggaran untuk meng-implementasikannya, dan pengembangan tersebut tidak dianggap sebagai prioritas utama (48%) jika dibandingkan dengan sum ber daya lainnya yang dimiliki oleh perusahan.

Perlakuan implementasi keamanan sistem sebagai pengeluaran rutin (*expenses*) ini, maka 59% organisasi global dan 84% perusahaan Inggris tidak pernah, jarang dan tidak tahu mengggunakan perhitungan *Return on Investment (ROI)* untuk biaya pengeluaran keamanan sistem informasi.

3. Pembahasan

Tingginya tingkat kesulitan dalam menghitung nilai manfaat yang *intangible* dalam implementasi keamanan sistem informasi, maka kajian ekonomi sederhana yang berdasarkan kriteria kualitatif dapat dipergunakan untuk sementara, walaupun banyak perusahaan tidak mempergunakan kriteria-kriteria keuangan dalam proses pengambilan keputusan yang berkaitan dengan investasi keamanan sistem informasi.

Dilain pihak, pimpinan puncak dan managemen madya suatu perusahaan dalam proses pengambilan keputusan selalu mempertimbangkan dampak finansialnya untuk setiap peng-gunaan dana internal perusahaan. Selain dampak finansial sebagai kriteria utama, kriteria berikutnya adalah memper-timbangkan pula kesesuaian (*strategic fit*) antara *resource*s yang akan diperoleh

dengan misi dan sasaran perusahaan dalam jangka menengah dan panjang, sehingga customer akan memperoleh manfaat atas perolehan *resources* tersebut.

Sudah menjadi suatu keharusan bahwa dalam melakukan investasi keamanan sistem informasi harus memperhatikan kriteria keuangan. Seorang CISO (*Chief Information Security Officer*) harus mampu menyakinkan *Chief Information Officer* (CIO) dan *Chief Finance Officer* (CFO) untuk menyetujui proyek implementasi keamanan sistem informasi, dan tidak hanya menentukan jenis-jenis proyek, menghitung masing-masing biaya, dan membelanjakan semua anggaran yang telah disetujui. Akan tetapi kemampuan yang harus dimiliki oleh CISO meliputi (i): pengkajian resiko yang dihadapi suatu perusahaan, (ii): menentukan kegiatan keamanan sistem informasi yang cocok dengan sasaran perusahaan. Hal tersebut dilaksanakan agar investasi di bidang keamanan sistem informasi dapat memberikan kontribusi kinerja keuangan dari suatu organisasi.

Kontribusi keamanan sistem terhadap kinerja perusahaan harus memperhatikan kondisi eksisting portfolio dari keamanan sistem informasi, sehingga kajian alternatif portfolio investasi dapat dilakukan secara terus menerus untuk menenuhi sasaran bisnis (*business objectives*) jangka pendek dan jangka panjang dari organisasi.

Managemen portfolio keamanan sistem informasi memberikan pendekatan yang terpadu dalam melakukan identifikasi, pemilihan, kontrol, evaluasi dan management investasi keamanan sistem. Dalam melakukan analisa kelayakan keamanan sistem, kajian terhadap performansi sistem eksisting dan identifikasi permasalahan investasi eksisting sangat diperlukan.

Hal ini dilakukan untuk memperbaiki kinerja keamanan sistem informasi melalui usulan investasi baru. Usulan tersebut

harus mempertimbangan faktor yang berkaitan dengan biaya, manfaat dan resiko. Adapun faktor-faktor tersebut harus dihitung berdasarkan atas ukuran-ukuran kuantitatif dan kualitatif seperti marginal analysis, ROI, ROSI, dan NPV.

3.1. Marginal Analysis

Marginal analisis merupakan salah satu cara pengambilan keputusan bagi CISO dengan membandingkan antara marginal manfaat yang dihasilkan dengan marginal biaya. Secara umum dapat dikatakan pula bahwa *Benefits(Q)* dapat diperoleh dari level keamanan sistem informasi yang diharapkan, dan sebanding dengan *Costs (Q)* atau biaya yang dikeluarkan untuk setiap level keamanan sistem informasi yang diinginkan.

Level tersebut sangat tergantung dari keputusan yang diambil atas persoalan yang dihadapi oleh organisasi. CISO mempunyai sasaran untuk memaksimalkan manfaat bersih (*net benefits*) dari implementasi keamanan sistem informasi.

N(Q) = B(Q)-C(Q)

Net benefits akan memiliki nilai tertinggi di level keamanan sistem informasi yang *optimum*.

Marginal benefits merujuk pada pertambahan manfaat (dapat berupa dollar dan rupiah) yang timbul atas pertambahan level dari *InfoSec*. Sedangkan *marginal cost* mengacu atas pertambahan biaya yang diperlukan atas pertambahan level dari *InfoSec*, dan *marginal net benefits* merupakan perubahan dari *net benefit* atas bertambahnya setiap level *infosec*. Akan tetapi *marginal net benefit* dapat pula diperoleh dari selisih antara *marginal benefit* dan *marginal cost.*

MNB(Q) = MB(Q) – MC(Q)

Pada kondisi level *InfoSec* optimal, kurva *marginal benefit* akan berpotongan dengan *kurva marginal cost* sehingga *marginal net benefitnya* mempunyai nilai nol dan *net benefit* mencapai nilai maksimal. Terkadang CISO dihadapkan dalam pengambilan

keputusan untuk mengajukan proposal/investasi tambahan dalam implementasi keamanan sistem informasi. Marginal analysis merupakan *prelimanary tool* dalam mengkaji keputusan tersebut. CISO harus mengadopsi keamanan sistem informasi baru jika tambahan biaya investasi akan menghasilkan manfaat lebih besar dari biaya yang dikeluarkan.

3.2. Return on Investment (ROI)

Untuk bentuk organisasi yang bersifat publik dan privat, metoda yang dipergunakan dalam menentukan layak-tidaknya suatu investasi keamanan informasi ditunjukkan oleh tingkat pengembalian atas uang yang dibelanjakan. Masih banyak organisasi mempergunakan metoda *Return on Investment (ROI)* untuk mengevaluasi investasi keamanan sistem informasi. ROI dipergunakan untuk pengukuran tingkat pengembalian modal, biasanya berkaitan dengan keuntungan atau penghematan biaya atas biaya yang telah dikeluarkan atau diinvestasikan. Selain itu, ROI dipergunakan untuk mengetahui seberapa baik asset yang telah dibeli dalam memberikan keuntungan. Kebanyakan ROI dipergunakan sebagai tolok ukur atas rencana bisnis atau proposal yang akan dikembangkan, sehingga proyek tersebut akan memberikan kontribusi besar terhadap entitas suatu perusahaan atau organisasi.

Persetujuan proposal tersebut didasarkan atas hubungan antara biaya yang dikeluarkan dengan manfaat yang dihasilkan. Semakin besar manfaat yang dihasilkan atas biaya yang dikeluarkan maka semakin besar pula nilai tingkat pengembalian modal.

3.3. Konsep Time Value of Money

Banyak perusahaan mempergunakan satu atau lebih ukuran keuangan yang terdiri atas, (i): Payback Period. Ukuran

keuangan ini menentukan waktu yang diperlukan agar manfaat yang diperoleh dan biaya yang dikeluarkankan seimbang, (ii): Net Present Value. Menilai manfaat yang dihasilkan di masa datang kedalam nilai uang saat sekarang, (iii): Internal Rate of Return merupakan manfaat yang dinyatakan dalam tingkat suku bunga.

Suatu organisasi yang akan melakukan investasi keamanan sistem informasi akan melibatkan banyak pilihan, maka *time value of money* dijadikan landasan dalam proses pengambilan keputusan. Teknik yang berkaitan dengan *time value of money* dikenal sebagai teknik analisa *discounted cash flow (DCF)* dengan menggunakan dua kriteria, yakni *Net Present Value (NPV)* dan *Internal Rate of Return (IRR*).

a. Present Value

Present value dari *cash flows* masa datang merupakan hubungan antara nilai investasi keamanan sistem informasi yang ditanamkan sekarang pada tingkat suku bunga tertentu dengan *cash flows* yang diperoleh di masa datang, sehingga nilai investasinya akan tertutupi. Untuk bidang keamanan sistem informasi, *cash flows* diperoleh dengan melakukan kuantifikasi atas manfaat yang diperoleh dari penggunaan keamanan sistem tersebut tersebut. Kuantifikasi manfaat dapat dilakukan dengan membandingkan *opportunity lost* yang terjadi jika tidak menggunakan keamanan sistem.

Manakala selisih *(Net)* antara nilai investasi dengan nilai sekarang dari proyeksi *cash flows* bernilai lebih besar dari nol (NPV > 0) maka investasi tersebut harus diterima (rumus-a). Jika nilai NPV lebih kecil dari nol maka investasi tersebut harus ditolak.

$$\text{NPV} = \sum_{t=1}^{n} \frac{\text{Cash flow}_t}{(1+i)^t} - \text{Investasi}_{t=0}$$

dengan,

NPV = Net Present Value

n = Perioda

i = Discount Rate

Rumus (e) menunjukkan bahwa NPV tersebut memperhitungkan *discount rate* sebagai faktor resiko atau ketidakpastian dari proyeksi *cash flows*, sehingga proyeksi *cash flows* harus dilakukan penyesuaian.

b. Internal Rate of Return (IRR)

Internal rate of return (IRR) adalah tingkat pengembalian pada keadaan NPV bernilai nol (rumus-e). Tingkat pengembalian dalam kriteria IRR tidak tergantung dari tingkat suku bunga yang berlaku (i), kecuali berkaitan langsung dengan *cash flows*. Oleh sebab itu, tingkat suku bunga (i) dalam rumus-e menjadi nilai IRR yang dihitung berulang-ulang agar diperoleh NPV=0.

Suatu investasi akan ditolak jika nilai IRR lebih kecil dari tingkat suku bunga. Sebaliknya, investasi akan diterima kalau nilai IRR lebih besar dari tingkat suku bunga yang berlaku.

3.4. Return on Security Investmen (ROSI)

Ditahun 2000 dan 2001, beberapa peneliti di Universitas Idaho-USA telah membuat rumusan untuk menghitung *Return on Investment* bagi keamanan sistem informasi. Rumusan tersebut dikenal sebagai *Return on Security Investment* (ROSI).

Para peneliti awalnya ingin menguji perhitungan teoristis dengan *actual cost* di dalam jaringan yang telah diletakkan pengangkat *Intrussion Detection System (IDS)* dengan sebutan *Hummer*. Perangkat akan memberikan peringatan dini manakala terdapat pola serangan yang dilakukan oleh *hacker*. Dari perhitungan teoritis, penentuan *tangible asset* seperti jaringan infrastuktur diukur dalam dollar dan *intangible asset* diukur dengan nilai relatif. Sedangkan *actual cost* dihitung dari rumusan yang telah ditentukan untuk bermacam-macam jenis serangan *hacker*.

Dari penilaian tersebut maka para peneliti memperoleh perhitungan biaya atas kerusakan yang dilakukan oleh *hacker* yang

terjadi beberapa kali, dan dikenal sebagai *Annual Lost Expectancy* (ALE). Adapun rumusan ROI yang menggunakan IDS sebegai *security defence* adalah :

(ALE x IDS Efficiency) - Cost of IDS = ROSI

Selain itu, mereka memperkirakan bahwa jaringan yang diserang akan mengalami kerugian sebesar US$ 100.000, untuk biaya IDS US$ 40.000 dengan efektivitas sebesar 85%. Dari perhitungan tersebut maka ROSI yang diperoleh sebesar US$ 45.000.

Para peneliti mengidentifikasi juga bahwa bertambahnya investasi sistem keamanan informasi secara gradual tidak akan menaikkan nilai ROSI terus menerus. Hal ini ditunjukkan dari kurva *smokestack*. Nilai terendah dari sumbu tegak dari kurva s*mokestack* (sumbu *survivability*) mengidentifikasikan bahwa perusahaan sangat rentan terhadap serangan keamanan sistem. Sedangkan perusahaan yang tidak berpengaruh terhadap *security breach* akan mempunyai nilai *survivability* yang besar.

Kondisi *survivability* yang mempunyai laju kenaikan lebih cepat dibandingkan laju kenaikan nilai investasi keamanan sistem. Pada titik tertertu, laju kenaikan *survivability* akan lambat seiring bertambahnya nilai investasi. Kurva *smokestack* ini konsisten dengan kurva *marginal net benefit* (MNB) seperti yang ditunjukkan pada gambar 3-3B dan 3-3C, dimana kurva *marginal net benefit* akan bernilai negatif setelah mencapai investasi keamanan sistem informasi yang optimal, atau kurva *net benefit* akan menurun seiring bertambahnya investasi. Dengan kata lain, dengan terus bertambahnya investasi setelah *optimal security investment* terlewati, *survivability* terhadap serangan akan bertambah tetapi laju pertambahannya akan turun atau disebut sebagai *law of diminishing ROSI*.

Selanjutnya rumus-(f) mengalami penyederhanaan menjadi :

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

dimana,

T = Biaya perangkat intrusion detection system (IDS)

E = Penghematan/Keuntungan yang diperoleh dari pemakaian IDS terhadap sejumlah serangan

R = Biaya tahunan untuk memperbaiki keadaan dari sejumlah sejarah.

Dari persamaan (g) akan diperoleh Annual Loss Expetancy (ALE) :

$$R - (ALE) = ROSI$$

Untuk menentukan *return on security investment* (ROSI), cukup mengurangkan kemungkinan kerugian dalam satu tahun (ALE) dari biaya tahunan untuk memperbaiki dari serangan (R). Untuk memperjelas hasil rumus (f), (g) dan (h) dapat diilustrasi-kan sebagai berikut : Sebuah perusahaan jasa pembiayaan keuangan memutuskan untuk menggunakan teknologi *wireless remote access* untuk pegawainya di Virtual Private Network (VPN), sehingga biaya untuk akses *dial-up* akan berkurang. Akan tetapi pemanfaatan *wireless remote access* memungkinkan *security breach* lebih besar terhadap *unauthorized access to confidential corporate information*. Sebuah pengamanan dipergunakan dengan proteksi dilakukan dengan mekanisme security terpisah (*Ipsec tunnel*) yang berkerja pada *wireless link* dan *VPN gateway* sehingga proteksi akan diberikan dari ujung-ke-ujung. Selain itu, diperlukan *updated anti-virus* di *VPN client* sebesar Rp. 2.5 Milyar (efektifitas 85% di pengujian setempat). Dengan adanya *wireless remote access* akan meningkatkan produktifitas pegawai sekitar Rp. 10 milyar dan mengurangi biaya akses *dial-up* sebesar Rp. 2.5 milyar. Diasumsikan pula bahwa perusahaan tersebut memiliki asset sekitar Rp. 2 Trilyun, dan diperkirakan bahwa kerugian asset senilai 0.1% jika terjadi serangan keamanan sistem informasi.

Dari data internal diperoleh bahwa rata-rata terjadinya

security breach sebanyak 3 kali per tahun.
Ilustrasi perhitungan :

ALE = Nilai Asset (Rp. 2 Trilyun) x Faktor Kerugian (0.1%) x Kejadian per tahun (3)
= Rp. 6 Milyar
E = {ALE (Rp. 6 Milyar) x Effektifitas (0.85)} + {Meningkatnya Produktifitas (Rp 4 Milyar)+ Penghematan biaya akses *Dial-up* (Rp.2.5 M)}
E = Rp. 11.6 Milyar
ROSI = E (Rp. 11.6 Milyar) - Biaya Perangkat Pengaman (Rp.2.5M)
= Rp. 9.1 Milyar

Dari ilustrasi tersebut di atas maka implementasi *wireless remote access* dan investasi keamanan sistem informasi sebesar Rp. 2.5 M, akan memberikan ROSI senilai Rp 9.1 Milyar.

Dalam melakukan asumsi tersebut diatas, CISO harus mampu dan yakin dalam membuat perhitungan atau meng-kuantifikasi ancaman-ancaman kedalam angka. Termasuk didalamnya membuat statistik *security breach* yang terjadi di dalam perusahaan, menghitung probabilitasnya dan effektifitas alat pengaman jika terjadi serangan sesungguhnya.

3.5. Real Option Model

Perkembangan dari *security breach* menjadi semakin komplek dan sulit untuk diprediksi kapan akan terjadi. Akibatnya CISO menghadapi ketidakpastian (*unceratinty*) yang tinggi. Ketidakpastian ini harus diatasi dan harus dapat dikapitalisasi agar dapat diperoleh manfaat yang besar. Pendekatan yang dilakukan untuk menghadapi ketidakpastian tersebut dapat menggunakan model *real options*. Model ini banyak dipergunakan untuk menilai

option yang diperdagangkan di lembaga pasar modal. *Option* memiliki kesamaan dengan layanan yang dijual oleh lembaga asuransi untuk melindungi obyek dari segala bentuk perusakan/perubahan-nilai dalam jangka waktu tertentu, sehingga resiko yang dihadapi dipindahkan ke pihak ketiga. Sebagai contohnya asuransi rumah, asuransi jiwa dan asuransi kendaraan. Sedangkan obyek dari options sangat bervariasi mulai dari saham, mata uang, Treasury Bill,emas, minyak & gas bumi dan lain-lain.

Options memberikan hak kepada pemilik *option* untuk melakukan sesuatu, dan pemilik berhak untuk menjualnya (*exercise right*) dengan pembelian *options* dilakukan dimuka. Terdapat dua jenis *option*, yakni *option* untuk membeli (*call options*) dan *option* untuk menjual (*put options*).

Call options memberikan hak kepada pemilik untuk melakukan investasi dengan biaya dibayar dimuka (*excercise price*) dan dapat dijual sebelum dan pada saat jatuh temponya (*maturity*). Sedangkan *put option* memberikan kesempatan untuk membatalkan investasi atau menjual kembali investasi tersebut pada nilai yang telah ditentukan diawal, pada saat atau sebelum terjadinya jatuh tempo.

Sebagai ilustrasinya dari *real options* (*ilustrasi dimodifikasi dari* [20]) adalah sebagai berikut: sebuah perusahaan jasa pembiayaan keuangan telah meng-anggarkan biaya untuk keamanan sistem informasi senilai Rp. 2.5 Milyar, dan meliputi (i): Rp. 1.5 Milyar untuk pembelian perangkat keras keamanan sistem (seperti *firewall*, proteksi fisik di masing-masing komputer). Anggaran ini sudah mendapatkan persetujuan dari *Chief Financial Officer* (CFO) selaku pimpinan CISO sehingga hak tersebut dapat dianggap sebagai *call options* dengan *excercise price* Rp. 1.5 Milyar, dan pada saat akan dibelanjakan maka option tersebut akan jatuh *maturity*-nya, (ii): Rp. 1 Milyar diperuntukkan keperluan

mendadak yang berkaitan dengan keamanan sistem informasi dan harus memperoleh persetujuan setiap akan dikeluarkan. Anggaran dapat dipergunakan untuk memperbaiki keamanan sistem seluruh perusahaan dengan cara men-*outsourcing*-kan ke pihak ketiga. Sedangkan pihak ketiga memiliki kebijakan untuk menerima kontrak keamanan sistem selama satu tahun dengan nilai Rp. 1 Milyar. Manakala kontrak telah ditandatangani untuk satu tahun maka nilai kontrak tidak dapat dihitung *prorata* jika diberhentikan atau ditunda ditengah jalan. Untuk anggaran Rp. 1 Milyar dapat dianggap sebagai *put option*.

Dari ilustrasi tersebut di atas maka *option valuation* dapat dihitung dengan menggunakan model *binomial* sederhana, selain model *Black-Scholes* yang memiliki kompleksitas tinggi tidak dibahas dalam karya ilmiah ini.

Hampir semua proyek investasi sangat berkaitan dengan fleksibilitas CISO dan CFO terhadap reaksi atas perubahan lingkungan keamanan sistem informasi dan lingkungan usaha suatu perusahaan. Hal ini memungkinkan mereka untuk menyesuaikan strategi investasi keamanan sistem sesuai dengan kondisi lingkungan dan sasaran bisnisnya. Dari kondisi tersebut, evaluasi proyek investasi dapat mengunakan metoda *real option*s yang dianggap sebagai teknik perhitungan keuangan moderen. Untuk teknik tradisional yang hanya mengenal keputusan untuk investasi atau tidak investasi, maka teknik tradisional ini menggunakan *discounted cash flow*s untuk menghitung *present value*, seperti teknik NPV, IRR, ROI dan ROSI.

Dua teknik terakhir (ROI dan ROSI) dikategorikan sebagai metoda tradisional, mengingat kedua teknik tersebut dibutuhkan investasi yang mempunyai *economic life* terbatas. Akibatnya, *discounted cash flow* tetap harus digunakan untuk menghitung nilai *economic life*-nya, walaupun dalam pembahasan bagian sebelum-nya *economic life* untuk ilustrasi ROSI hanya diperhitungkan satu

tahun.

Perbedaan penting antara *tradisional valuation* denga *real option* adalah faktor resiko atau ketidakpastian (*uncertainty*) yang masuk dalam perhitungan. Untuk lingkungan yang memiliki *uncertainty* sangat tinggi, model *real option* menjadi lebih bernilai sehingga *option value* menjadi lebih besar.

Present value suatu investasi dapat dihitung dengan tepat manakala investasi telah dilaksanakan seiring berjalannya waktu sehingga ketidakpastian (*uncertainty*) telah diketahui dengan pasti. Untuk lingkungan dengan gejolak perubahan sangat tinggi (*high volatile*), nilai proyek investasi menjadi sangat besar sehingga NPV yang dihasilkan menjadi lebih besar. Hal ini terjadi karena *real option value* membunyai nilai besar. Sedangkan dalam kondisi volatilitas rendah, NPV yang dihasilkan sangat kecil karena nilai *option* berharga kecil atau nol.

Sampai saat ini *volatility* dianggap sebagai hal yang merugikan sehingga dalam perhitungan *discounted cash flows*, penyesuaian dilakukan dengan memberikan *discount rate* yang lebih tinggi (rumus-e) untuk teknik tradisional. Akibatnya proyek investasi keamanan sistem informasi dibentuk dari resiko yang sudah diprediksi diawal dan tidak akan dirubah selama proyek tersebut berlangsung.

Model *real options* berkaitan erat dengan teknik tradisional yang keduanya menggunakan pendekatan *discounted cash flows* dan fleksibilitas dari *uncertainty*. Sedangkan dalam teknik tradisional, fleksibiltas untuk mempertimbangkan *uncertainty* diasumsikan tidak ada atau nol. Akibatnya model *real options* akan menghitung NPV yang telah diperluas (*extended NPV*) yang terdiri dari proyek investasi tradisional (NPV) dan proyek *option value*. Sedangkan *option value* dapat diperoleh dari (i): kondisi *option to wait* dalam penundaan investasi sampai keadaan ekonomi membaik, (ii): kondisi *option to stage investment* dalam kondisi

untuk tetap melakukan investasi, (iii): kondisi *option to shut down*, dan (iv) kondisi *option to switch*.

Akibatnya, *uncertainty* dianggap hal positif dan harus ditambahkan dalam traditional *valuation* (option value-C1 dari gambar 4-3), dan *uncertainty* sebagai pengurang NPV dihilangkan (negatif PV atau posisi garis *A1-X1* dibawah sumbu A).

Adapun kondisi *option to wait, option to shut down* dan *option to switch* untuk investasi keamanan sistem akan mempengaruhi pergerakan garis *A-X* (A adalah PV proyek dan X adalah *excercise price*) keatas dan kebawah sehingga *volatility* atas *security breach* akan memberi keuntungan terhadap perkembangan lingkungan yang ditunggu. Akibatnya, penantian tersebut akan menurunnya biaya investasi untuk PV, dan hilangnya pendapatan. Tetapi *exercise real option*s lebih awal tentunya akan memberikan keuntungan yang lebih baik.

4. Penutup

Terjadi perubahan mendasar dalam menjalankan organisasi dari kegiatan tradisional ke organisasi yang terhubung dengan internet (*e-business*), sehingga asset perusahaan yang berupa informasi harus tetap terjaga dan terpelihara terhadap segala perubahan tersebut. Pemeliharaan informasi tak terbatas terhadap gangguan yang dilakukan dari pihak luar, tetapi juga harus mempertimbangkan gangguan yang dilakukan oleh pegawai perusahaan dan pengendalian arus data di dalam jaringan perusahaan. Pengamanan terhadap gangguan keamanan sistem informasi harus secara proaktif dilakukan baik oleh CISO maupun kebijakan perusahaan, jika tidak mau kehilangan kapitalisasi pasar akibat pemberitaan publik.

Walaupun terdapat hubungan antara strategi bisnis dan kondisi perusahaan dalam mengembangkan keamanan sistem informasi, organisasi harus mulai memperlakukan keamanan

sistem informasi sebagai bagian dari investasi. Dampak ekonomi (*financial impact*) perusahaan yang digunakan sebagai kriteria pengambilan keputusan dalam pemanfaatan data internal dapat menggunakan teknik tradisional dan moderen dalam melakukan perhitungan investasi keamanan sistem informasi.

Pemanfaatan model *real options* dapat memberikan kontribusi di organisasi untuk membantu fleksibilitas CISO dan CFO dalam mengambil keputusan investasi keamanan sistem di lingkungan *volatility* tinggi. Selain itu, fleksibilitas management untuk melakukan *Option to switch, option to stage investment* dan *options* lainnya memberikan fleksibilitas bagi organisasi untuk mengkaji posisi *net benefit* atas *information security* atau *survivalibility* nya sudah mencapai titik optimum atau belum dengan bertambahnya *security investment*.

Daftar Pustaka

PriceWaterHouse-Coopers, "*Information Security Breaches Survey 2002 : Technical Report*", April 2002. http://www.security-survey.gov.uk/

Computer Security Institute, "*CSI/FBI Computer Crime and Security Survey 2003*", Eight Annual. http://www.gocsi.com/

L.A. Gordon dan M.P. Loeb, "*Economics Aspect of Information Security*", Rainbow Technologies, v.2.1, Agustus 2001.

K. Champbel, L.A. Gordon dan M.P. Loeb, Lei Zhou, "*The Economics Cost of Publicly Announced Information Security Breaches : Empirical Evidence from The Stock Market*", Working Paper, Mei 2001.

Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan, "*The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developer*", School of Management, The University of Texas, Dallas, Pebruari 2002.

Ernst & Young, "*Global Information Security Survey 2003*". http://www.ey.com/global

Eva Kuiper, "The Reality about Investing in Information Security",*Security Investment Justification*, Hewlet-Packard, Pebruari 2003. http://www.hp.com/

Michael R. Baye, "*Managerial Economics & Business Strategy*", McGraw-Hill Higher Education, Edisi-3, 2000.

Steve Foster dan Bob Pacl, "Analysis of Return on Investment for Information Security", A White Paper, Getronics. http://www.getronics.com/us

Q1Labs, "Illegal Peer-to-Peer File Sharing: Are You Protected", *Q1 Labs White Paper*, Maret 2003. http://www.q1labs.com/

L.A. Gordon dan M.P. Loeb, "*Real Options and Security : The Wait-and-See- Approach*", Computer Security Journal, Vol.19, No.2, 2003.