IMPLEMENTASI KEAMANAN SISTEM INFORMASI DENGAN MODEL REAL OPTION MODEL

Oleh :

Ronal Watrianthos
Dosen Prodi Manajemen Informatika, AMIK Labuhanbatu
Rantauprapat, Medan; ronaw@amik-labuhanbatu.ac.id

Abstract

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

Walaupun terdapat hubungan anatara strategi bisnis dan kondisi perusahaan dalam mengembangkan keamanan sistem informasi sebagai bagian dari investasi. Dampak ekonomi(Financial impact) perusahaan yang di gunakan sebagai kriteria pengambilan keputusan dalam pemanfaatan data internal dapat menggunakan teknik tradisional dan modren dalam memlakukan perhitungan invesitas kemanan 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 tinggu. Selain itu, fleksibilotas management untuk melakukan option to switch, option to stage investment dan options lainnya memberikan fleksibilitas bagi organisasi untuk menkaji posisi net beneft atas information security atau survivalibility-nya sudah mencapai titik optimun atau dengan bertambahnya security investment.

Keyword : CISO, NPV, CCFO, Model

I. PENDAHULUAN

Suatu perubahan 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 akusisi sumber daya tersebut. Hal ini tidak terkecuali dalam aktivitas yang berkaitan dengan ***information security.***

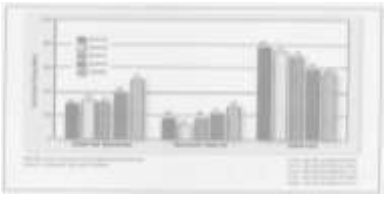
Model-model ekonomi tradisional untuk mengkaji tingkat pengembalian invenstasi atas pengeluaran perusahan (*expenditures*) dibidang *information seurity* masih menjadi bahan perdebatan, mengingat aspek teknis dari *information security* (misal: teknik enkripsi dan *intrusion detection system*) sangat 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 secaraa nyata. Jika model NPV tersebut dipergunakan maka perubahan manfaat (*incremental benefits*) yang terus menerus dari implementasi information security harus terukur. Sedangkan komponen terukur dibidang *information security* baru sebatas total biaya pengeluaran untuk total pembelian aset fisik dari *informaation security*.

II. LANDASAN 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 diinggris dan US telah terjadi perubahan,yakni dengan memberdayakan kemampuan internet untuk melakukan aktivitas *e-business* [1]. Pemanfaatan internet ini memberi dampak langsung terhadap keamanan sistem informasi dan menjadikan internet sebagai pintu gerbang serangan kesistem informasi suatu organisasi.



Gambar 1.
Koneksi Internet sebagai serangan Sistem Informasi

Hasil survey dari tahun 1999 sampai 2003 yang dilakukan CSI/FBI terhadap respon-den di USA memperlihatkan peningkatan serangan sistem informasi organisasi melalui internet (gambar 2-1). Sedangkan serangan keamanan informasi menggunakan *internal system* dan *remote dial-in* mengalami penurunan. Hal tersebut didukung dengan hasil servey diperusahaan inggris, dimana internet dipergunakan untuk mengirim e-mail. Tercatat 77% total perusahaan dan 99% korporasi besar menggunakan e-mail sebagai bentuk korespondensi antar pegawai.

Selain itu diketahui pula bahwa 69% total perusahaan dan 92% perusahaan besar yang disurvey memberikan kesempatan kepada pegawainya untuk mempergunakan akses *web* (gambar 2-2). Yang menarik dari hasil tersebut menunjukkan pula, hanya 13% perusahaan yang menerima transaksi perdagangan dengan menggunakan *customer online*. Dengan kecenderungan perusahaan didunia untuk melakukan transaksi perdagangan secara *online* antara institusi bisnis dengan kastamer (B2C) atau antara institusi bisnis dengan institusi bisnis lainnya (B2C), maka aspek ekonomi dari keamanan sistem informasi mulai menjadi pokok permasalahan.

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 invenstasi yang berkaitan dengan keamanan sistem informasi [3], 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 aktivitas *e-business*. Survey terhadap lebih dari 1400 organisasi yang dilakukan pada tahun 2003 diseluruh dunia oleh Ernst & Young, mengidikasikan bahwa intensitas ancaman sistem informasi paling tinggi dalam 12 bulan kedepan diakibatkan olieh *virus* (Gambar 2).
Virus mempunyai intensitas ancaman keamanan sistem informasi yang paling tinggi (skala intensitas antara skala 3 dan 4).

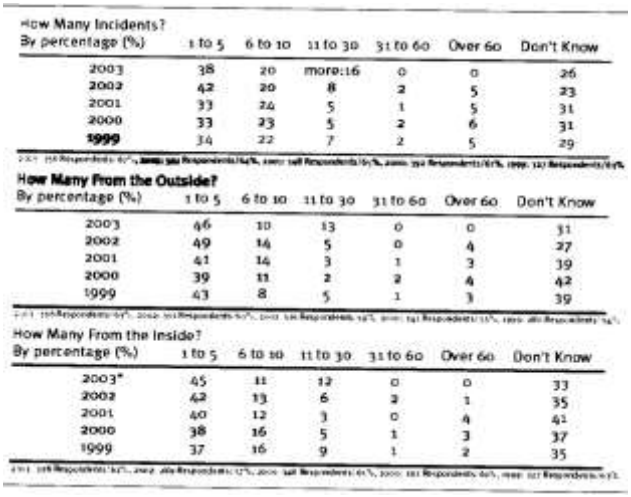
Relative Intensity of Threats over the next 12 months?	Mean: Low 1	2	Mod. 3	4	High 5
Major virus or worm			●		
Employee misconduct involving information systems		●			
Distributed Denial of Service (DDoS) attack		●			
Loss of customer data privacy/confidentiality		●			
Amateur hackers or "Script Kiddies"		●			
Theft of proprietary information or intellectual property		●			
Consultants/vendors who have access to info systems		●			
Former employee misconduct involving info systems		●			
Natural disasters		●			
Business partner(s) misconduct involving info systems		●			
Competitor espionage		●			
Political "hacktivism" or cyber protest		●			
Cyber-terrorism — foreign-based		●			
Cyber-terrorism — domestic-based	●				
Non-nuclear terrorist attack	●				
Cyber War	●				
Foreign government espionage	●				

Gambar 2. Intensitasi Ancaman dalam Keamanan Sistem Informasi untuk Tahun Mendatang

Sedangkan intensitas ancaman urutan kedua akibat oleh status kepegawaian seseorang, dan diikuti dengan intensitas urutan ketiga yakni distributed Deniel of Servicess attack (DdoS) (gambar 2).

Hasil temuan tersebut diatas sangat konsisten dengan servey yang dilakukan diinggris tahun 2002 dan di USA 2003, dimana virus dan pegawai perusahaan mendominasi semua pelanggaran keamanan sistem. Untuk ancaman yang dihadapi oleh semua skala industi diinggris 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 *haker* di *website* (11%).

Jika dibandingkan dengan hasil survey dinggris ditahun 2002, 2003 dan tahun 1998, pelanggaran keamanan sistem informasi terjadi peningkatanyang sangat berarti. Sebagai contohnya, ditahun 1998 pelanggaran telah dialami oleh 18% responden. Selanjutnya terjadi peningkatan lebih dari dua kali ditahun 2002 yakni 44% untuk semua skala industri, sedangkan skala industri besar telah dialami oleh 78% responden.



How Many Incidents?

By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003	38	20	more:16	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29

How Many From the Outside?

By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39

How Many From the Inside?

By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003*	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35

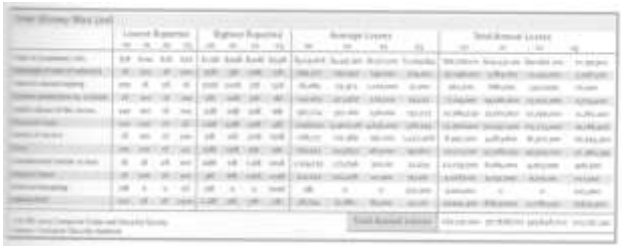
Gambar 4. Frekuensi Kejadian Pelanggaran Sistem Keamanan

Dari kejadian-kejadian pelanggaran sistem keaman informasi dan di USA dilaporkan bahwa frekuensi pelanggaran untuk kejadian kurang dari 6 kali dalam satu tahun lebih banyak dihadapi oleh setiap perusahan (gambar 4). Yang menarik dari hasil tersebut adalah tinggi-nya persentase organisasi yang tidak mengetahui frekuensi kejadian pelanggaran keamanan sistem informasi nya, baik yang berasal dari luar dan dari dalam organisai tersebut.

Dari kejadian tersebut menunjukkan bahwa *countinous improvement* terhadap sistem keaman informasi menjadi kebutuhan sangat vital untuk mengurangi frekuensi pelanggaran yang tidak diketahui jumlah dan asalnya.

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.



Gambar 5
Kerugian untuk Setiap Jenis Pelanggaran Keamanan Sistem

Ditahun 2003,CSI/FBI melaporkan bahwa 75% dari 530 responden mengalami kerugian atas pelanggaran keamanan sistem informasi, dan hanya 47% dari responden tersebut yang dapat menghitung kerugian tersebut [2]. Seperti diperhatikan pada gambar 5, *total annual losses* terbesar diakibatkan oleh pencurian informasi penting perusahaan yang mencapai US$ 70 juta. Kerugian tersebut telah mengalami penurunan lebih dari separuh kerugian, jika dibandingkan yang diakibatkan oleh kejadian yang sama ditahun 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 ditahun 2003 mengalami peningkatan lebih dari tiga kali dibandingkan dengan kejadian sama ditahun 2002, dan mengalami peningkatan lebih dari 14x jika dibandingkan ditahun 2001.

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

Dari kerugian keuangan yang diakibatkan dari beberapa jenis gangguan keamanan sistem informasi tersebut diatas, tercatat bahwa kurang dari seperti (33%) organisasi menutupi kerugian keuangan tersebut dengan kebijakan perusahaan masing-masig. Sedangkan 34% organisasi tidak menggunakan jasa asuransi unutuk mengatasinya. Sisanya (33%) masih tetap menjadi persoalan didalam organisasinya 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 keamanan tersebut.

Keterbatasan tersebut tidak hanya dihadapi oleh pengelolah perusahaan saja, tetapi juga oleh penyedia jasa asurasi.

2.4 Proses Investasi Keamanan Sistem Informasi

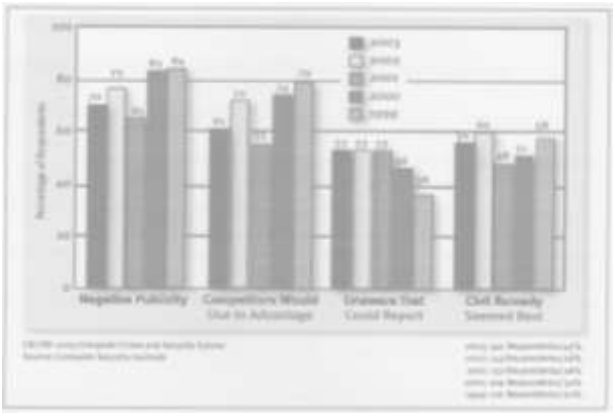
Biaya yang dikeluarkan untuk myembangun keamanan sistem informasi sampai saat ini masih dianggap sebagai pengeluaran rutin (*expenses*) sehingga pengeluaran biaya tersebut tidak menjadi prioritas utama dan tidak diperlukan sebagai investasi. Konsekuensinya, keperluan untuk mengembangkan keamanan sistem menjadi

kendala karena keterbatasan anggaran biaya. Hal itu ditunjukkan dari hasil survey global dimana 56% responden menghadapi keterbatasan anggaran untuk mengimplementasikannya, dan pengembangan tersebut tidak dianggap sebagai prioritas utama (48%) jika dibandingkan dengan sumber daya lainnya yang dimiliki oleh perusahaan. Perlakuan implementasi keamanan sistem sebagai pengeluaran rutin (*expenses*) ini, maka 59% organisasi global dan 84% perusahaan inggris tidak pernah, jarang dan tidak tahu menggunakan perhitungan *Return on Investment* (ROI) untuk biaya pengeluaran keamanan sistem informasi.

Terdapat beberapa alasan untuk tidak mempergunakan perhitungan ROI untuko pengeluaran biaya keamanan sistem , yakni (i): manfaat yang ditimbulkan dari pemanfaatan keamanan sistem bersifat intagible atau sukar diukur seperti hilangnya waktu untuk pegawai pada saat terjadi gangguan ;(ii): banyak profesional keamanan sistem memiliki latar belakang pendidikan teknis sehingga kemampuan untuk mengembangkan *Business case* sangat terbatas; (iii); komitmen managemen puncak sangat rendah terhadap keamanan sistem informasi dikala mereka belum menghadapi kejadian berat yang mempengaruhi kinerja suatu perusahaan; (iv) cara perhitungan ROI hanya dilakukan untuk melakukan kajian inventasi yang memiliki nilai yang cukup besar dan berkaitan langsung terhadap pendapatan/ *revenue* suatu perusahaan, sehingga untuk semua jenis expenses tidak diperlukan perhitungan tersebut.

2.5. Reaksi Portofolio Investor terhadap Security Breaching

Banyak perusahaan publik dan swasta yang tidak melaporkan kejadian gangguan keamanan sistemnya kepada publik atau kepihak berwajib. Keengganan untuk melaporkan kejadian tersebut disebabkan oleh dampak lanjutan yang akan dihadapi.



Gambar 3
Alasan Tidak Melaporkan *Security Breaching* bagi Organisasi di USA

Hasil CSI/FBI mengindikasikan bahwa pemberitaan negatif atas perusahaan menempati rangking pertama, jika kejadian pelanggaran sistem keamanan dilaporkan kepihak berwajib. Akibatnya pesaing akan mengambil keuntungan dari pemberitaan negatiftersebut sehingga *image* perusahaan maupun *brand identity* atas produk atau layanan yang dihasilkan menjadi taruhan bagi kelanjutan usaha perusahaan tersebut.

Pemberitaan negatif tentang *security breach*bagi perusahaan publik yang tercatat di bursa saham mempengaruhi performasi nilai saham untuk jangka pendek dan jangka panjan. Dampak tersebut dapat dipahami dengan menggunakan metode analisa *event study.*

a. Metodologi Event Study

Untuk pasar modal yang memiliki kondisi *Efficient Market Hypotheses* (EMH), segala bentuk informasi baru yang masuk kepasar modal dan berkaitan dengan pemberian emiten (*listed company*), maka *portfolio investor* akan melakukan penyesuaikan harga saham dengan cepat [8]. Penyesuain harga saham tersebut mencerminkan pengaruh informasi baru yang berkaitan dengan *security breach* termasuk didalamnya resiko-resiko yang mungkin akan timbul seperti *potential finalcial losses.*

Pengkajian terhadap (i): pergerakan harga saham disaat-saat pemberitaan *security breach* dan (ii): waktu terjadinya penyesuain harga, akan memberikan indikasi kepada publik apakah pemberitaan tersebut disebarkan secara terbatas atau luas. Jika harga saham perusahaan publik yang mengalami *security breach* terjadi penggerakan besar, yakni satu hari (H-1) sebelum diumumkan kepada publik (H), maka penggerakan besar harga saham untuk periode *event* tersebut mengindikasikan terjadinya *insider trading.*

Hal ini terjadi karena hanya beberapa *insider trader* yang memiliki informasi tersebut mengambil keuntungan terhadap kepentingan publik sehingga *insider trader* memiliki peluang besar untuk memperoleh tingkat keuntungan diatas rata-rata (*above-average-rate-of-return)* yang sangat besar. Jika harga saham bergerak secara normal sebelum diumunkan kepada publik, maka penggerak-normal harga saham tersebut diakibatkan oleh kegiatan transaksi jual-beli pada umumnya.

Above average of return atau abnormal rate of return untuk individu harga saham yang berreaksi atas *public announcemet* tidak akan memiliki makna, jika *return* dari agregat semua harga saham mengikuti pola yang saama. *Abnormal rate of return* dapat diformulasikan sebagai berikut.

Arit = Rit – Rmt .....(a)

Dimana,

Arit = *Abnormal Rate of Return* untuk Saham *i* selama kurun waktu *t*

Rit = *Rate of Return* untuk Saham *i* selama kurun waktu *t*

Rmt= *Rate of Return* untuk index pasar modal selama kurun waktu *t*

Sebagai contohnya, harga saham A mengalami penurunan harga sebesar 5% setelah diumumkan terjadinya *security breach,* sedangkan Index Harga Saham Gabungan (IHSG) untuk pasar modal jakarta (*Jakarta Stok Exchange)* mengalami kenaikan sebesar 2%. Dari informasi tersebut dapat dikatakan bahwa perubahan abnormal harga (*abnormal price hange)* untuk perioda *event* {0,+1} sebesar -7% (minus 7%) dan investor merespon pengumuman *security breach* sebagai sinyal negatif terhadap kinerja perusahaan yang memiliki potensi terjadinya kerugian keuangan jika tidak dapat diatasi.

Selain *abnormal rate of return,* dimungkinkan pula untuk mengkaji dampak keseluruhan terhadap pengumuman tersebut disekitar *event,* sehingga perhitungan *abnormal rate ohf return* disekitar *event* akanmenghasilkan *umulative abnormal return*(CAR).

$CARi = \sum_{t=1}^{n} A\,R_{it}$ .....(b)

Dari uraian diatas diperoleh dua pendekatan untuk mengamati perubahan harga abnormal disekitar saaat-saat pengumuman *security breach* untuk melihat penyesuaian harga, atau mengamati *abnormal rate of return* setelah sesaat diumumkan *security breach* untuk melihat kemungkinan investor memperoleh *above average rate of return* dalam kondisi *Semistrong Efficent Market Hypotheses.*

b. **Hasil *Event Study***

untuk mengetahui dampak yang dihadapi oleh emiten yang mengalami *security breach,* beberapa *event study* telah dilakukan meliputi *corporate security breach, Denial –of –Service* dan *internet security breach.* jenis *internet security breach* yang banyak dilakukan adalah serangan *Denial of service* (DOS). Penyerangan ini dilakukan dengan membuat *resources* yang dimiliki perusahaan menjadi tidak dapat beroperasi karena tidak adanya *resources* yang tersisa kepada *users* lainnya. Dalam lingkungan internet,DOS menyerang keserver perusahaan dan biasanya merupakan *web server* dan penyerang menjalankan program *ping* berulangkali sehingga menghabiskan *resources* di server.

Dari data statistik diperoleh bahwa publikasi serangan DOS yang dilakukan sejak 1 januari 1998 sampai 30 juni 2002 tercatat sebanyak 23 kejadian. Serangan tersebut terhadap perusahaan – perusahaan publik yang tercatat di New York Stock Exchange (NYSE) dan NASQAD *stock exchange*. *Event study* yang dilkukan terhadap 23 perusahaan publik untuk periode *event* {-1,0}, {-1,+1}, {-1,+5}, {-1,+10} dan {-1,+25} menunjukkan bahwa 48% publikasi yang berita tentang serangan DOS memberikan nilai *negatif abnormal rate of return* (AR).

Selanjutnya, 23 perusahaan publik tersebut dikelompokkan keperusahaan yang berbasis internet untuk bisnis intinya, dan perusahaan yang bisnis intinya tidak berkaitan langsung dengan internet. *Event study* terhadap kedua kelompok perusahaan publik menunjukkan bahwa perusahaan publik yang memiliki bisnis inti berkaitan langsung dengan internet memberikan nilai *negative abnormal return* lebih besar dibandingkan kelompok lainnya. Hal ini menunjukkan bahwa *portfolio investor* memberikan reaksi sangat *negative* terhadap perusahaan publik yang bisnis intinya berkaitan dengan*e-commerce* dan mendapatkan serangan *Denial of service.*

Perubahan harga saham tersebut diakibaatkan oleh ekspektasi investor terhadap nilai ekonomi perusahaan karena berkurangnya *cash flow* perusahaan yang dialokasikan u8ntuk memperbaiki keamanan sistem perusahaan setelah mengalami serangan DOS. Akibatnya. Perusahaan publik yang bisnis intinya berkaitan dengan internet harus memperlakukan *information security* sebagai bagian dari investasi, analisa invensitasi harus dilakukan, dan perlakukan keamanan sistem informasi sebagai *expenses* harus ditinggalkan.

Sedangakan *event study* terhadap perusahaan publik yang menghadapi *corporate information security breach* hanya membatasi permasalan pada dampak akses *illegal* terhadap informasi rahasia perusahaan (*unauthorized acces to confidential information),* dan dampak akses *illegal* trhadp informasi klasifikasi biasa (*unauthorized acces to non-confidential information)* [4]. Adapun yang termasuk dalam kategori informasi rahasia perusahaan adalah (i): data kredit card , (ii): data *customer* perusahaan, (iii): data penting perusahaan, (iv): informasi rahasia yang dikerjakan oleh pegawai. Sedangkan yang termasuk kategori informasi adalah (i): *virus,* (ii): *Denial of service* dan (iii): gangguan terhadap *website* perusahaan.

Event study dilakukan terhadap 43 perusahaan publik yang mengalami *corporate information security breach* sejak januari 1995 sampai Desember 2000 dengan perdandingan 11 *sampel* masuk kategori *unathorized acces confidential information* dan 32 *sample* sebagai kategori *unauthorized acces non-confidential information.*

Public unautcement untuk setiap perusahaan publik selanjutnya dianalisa dampak sekitar perioda *event* selama tiga hari atau {-1,+1}. Hasil pengamatan yang dilakukan oleh Champbel, Gordon dan Zhou menunjukkan bahwa perusahaan publik yang menghadapi *unaunthorized access non-confidential information* menhasilkan negatif CAR, yakni penurunan harga saham sebesar 0,7% setelah kejadian tersebut dipudlikasikan. Disamping itu perusahaan yang mengalami penurunan harga saham karena pelanggaran diatas sebesar dialami oleh 40.63% sampel.

Sebaliknya, penutrunan harga saham semakin besar (minus 5.5%) manakah kejadian yang berkaitan dengan *unauthorized access confidential information* dipublikasikan. Penurunan harga tersebut (negatif CAR) dialami oleh 63.6% perusahaan dalam kategori pelanggaran akses illegal informasi rahasia. Hal ini mengindikasikan bahwa *portfolio investor* sangat berkepentingan terhadap pelanggaran keamanan sistem perusahaan yang brrkaitan dengan akses illegal ke informasi rahasia perusahaan yang akan memberi keuntungan kepada pesaing perusahaan publik tersebut. Akibatnya, investor khawatir dengan publisitas tersebut akan dimanfaatkan oleh pesaing untuk menghilangkan *customer* maupun *partner* bisnisnya. Hal ini konsisten dengan hasil survey (lihat gambar 8), dimana pelaporan tersebut akan membawa dampak publisitas negatif bagi perusahaan dan akan dimanfaatkan oleh pesaingnya.

Sedangkan *event study* yang dilakukan oleh Cavusoglu, Mishra dan Raghunathan lebih banyak menguji *abnormal rate return* yang berkaitan dengan *internet security breach* dan pengembangan keamanan sistem baru untuk perusahaan. Lingkup *internet security breach* meliputi *Deniel of service* IT *failure* dan *security incident* lainnya.

Dari 66 perusahaan publik yang diuji untuk perioda *public announcement* dari 1 januari 1996 sampai 31 Desember 2001, perusahaan publik yang mengumumkan *internet security breach* mengalami penurunan harga saham sebesar 2.1% untuk perioda event {-2+2}. Penurunan harga saham tersebut setara dengan kerugian kapitalisasi pasar (*market capitalization)* sekitar US$1.65 miliyar untuk satu kali peristiwa.

Sedangkan perusahaan publik yang mengimplementasikan dan mengembangkan keamanan sistem informasi baru menunjukkan positif *abnormal rate of return* sebesar +1.36% atau setara dengan kenaikan kapitaalisasi pasar untuk perusahaan tersebut senilai US$ 1.06 miliyar [6]. Nilai tersebut diperoleh dari hasil *event study* untuk perioda {0,+1}.

Dengan kata lain, kenaikan kapitasi pasar bagi perusahaan yang mengimplementasikan keamanan sistem baru, mengindikasikan reaksi penyesuain harga saham yang dilakukan oleh *portfolio investor* atas sinyal yang dikeluarkan oleh emiten. Sinyal tersebut dianggap bahwa perusahaan mempunyai komitmen jelas terhadap pencegahan *security breach,* dan berusaha meminimalisasi *opportunitty lost* jika terhadap *security breach* dikemudian hari.

Sebaaiknya, emiten yang lalai dalam melakukan *cotinious improvement* terhadap keamanan sistem informasi diperusahaan akan memperoleh pinalti dari *portfolio investor* berupa kerugian dalam kapitalisasi pasar karena penurunan harga saham yang tercatat di bursa saham. Kerugian tersebut masih ditambah dengan kegiatan yang diakibatkan oleh *average cost* yang dikeluarkan untuk memperbaiki sistem informasi untuk setiap kejadian dari masing –masing jenis *security breach.*

III. PEMBAHASAN

Tingginya tingkat kesulitan dalam menghitung nilai manfaat yang *intangible* dalam implementasi keamanan sistem informasi, maka kajian ekonomi sederhana yang berdasarkan kriteria kualitatif dapat dipegunakan 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 perusahan dalam proses pengambilan keputusan selalu mempertimbangkan dampak finalsialnya untuk setiap pengguna dana inuternal perusahaan. Selain dampak finalsial sebagai kriteria utama, kriteria berikutnya adalah mempertimbangkan pula kesesuaian (*strategic fil*) antara *resources* yang akan diperoleh dengan misi dan sasaran perusahaan dalam jangka menengah dan panjang, sehingga customer akan memperoleh *recources* tersebut.

Sudah suatu menjadi keharusan bahwa dalam melakukan investasi keamanan sistem informasi harus memperhatiakan kriteria keuangan.

Seorang CISO (*Chief information Security Officer)* haarus mampu menyakinkan *Chief Information Officer* (CIO) dan *Chief Information 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 sasarn perusahaan. Hal tersebut dilaksanakan agar intestasi dibidang keamanan sistem informasi dapat memberikan kontribusi kinerja keuangan dari suatu organisasi.

Kontribusi keamanan sistem terhadap kenarja perusahaan harus memperhatiakan kondisi eksisting portfolio dari keamanan sistem informasi, sehingga kajian alternatif potrfolio invenstasi dapat dilakukan secara terus-menerus untuk memenuhi sasaran bisnis (*business objektives*) 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 performasi sistem eksisting dan indifikasi permasalahan invenstasi eksisting sangakkt diperlukan.

Hal ini dilakukan untuk memperbaiki kinerja keamanan sistem informasi melalui usulan invenstasi baru. Usulan tersebut harus mempertimbangkan faktor yang berkaitan dengan biaya, mamfaat dan resiko. Adapun faktor-faktor dan kualitarif seperti marginal analysis, ROI,ROSI dan NPV.

3.1 Marginal Anlysis

Marginal analisis merupakan salah satu cara pengambilan keputusan bagi CISO dengan membandingkan antara marginal manfaat yang dihasilkan dengan marginal biaya. Sebagai contohnya, Gambar 3-3A menunjukkan total manfaat yang dihasilkan dari setiap unit variabel keamanan sistem informasi (*Infoces Level*)yang dikelola oleh COSI. 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 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 benefist*) dari implementasikan keamanan sistem informasi.

$N(Q)= B(Q)-C(Q)$ .....(c)

Net benefits akan memiliki nilai tertinggi dilevel informasi yang *optimum.*

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

$MNB(Q)=MB(Q)- MC(Q)$.....(d)

Pada kondisi level *Infosec* Optimal, kurva *marginal* akan berpotongan dengan *kurva marginal cost* sehingga *marginal net benefistnya* mempunyai nilai nol dan *net benefit* mencapai nilai maksimal. Terkadang CISO dihadapkan dalam pengambilan keputusan untuk mengajukan proposal/invenstasi tambahan dalam implementasi keamanan sistem informasi. Marginal analysis merupakan *prelimanary tool* dalam mengkaji keputusan tersebut. CISOharus mengadopsi keamanan sistem informasi baru jika tambahn biaya investasi akan menghasilkan manfaat lebih besar dari biaya yang dikeluarkan.

3.2 Return on Investment (ROI)

Untuk membentuk organisasi yang bersifat publik dan privat, metode yang dipergunakan dalam menentukan layak-layaknya suatu investasi keamanan informasi ditunjukkan oleh tingkaut pengembalian atas uang yang

dibelanjakan. Masih banyak organisasi mempergunakan metode *Return on Investment (ROI)* untuk mengevaluasikan keamanan sistem informasi . ROI dipergunakan untuk pengukuran untuk pengukuran tingkat pengembalian modal biasanya berkaitan dengan keuntungan atau penghematan biaya atas biaya yang tela dikeluarkan atau diinvestasikan. Selain itu, ROI dipergunakan untuk mengetahui seberapa baik asset yang telah dibeli dalam memberikan keuntungan. Kebanyakkan 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 ytersebut didasarkan atas hubungan antara biaya yang dikeluarkan dengan manfaat yang diihasilkan. 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 dikeluarkan seimbang (ii): Net Present Value. Menilai manfaat yang dihasilkan dimasa datang kedalaman nilai uang saat sekarang, (iii): Internal Rate of Return merupakan manfaat yang yang dinyatakan dalam tingkat suku bunga.

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

a. Present Value

Present value dan *cash flows* masa datang merupakan hubungan antara nilai investasi keamanan sistem informasi yang ditamankan sekarang pada tingkat suku bunga tertentu dengan *cash flows* yang diperoleh oleh dimasa 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 informasi tersebut. Kuantifikasi manfaat dapat dilakukan dengan membandingkan *opportuninity lost* terjadi jika menggunakan keamanan sistem.

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

$$\text{NPV} = \sum_{t=1}^{n} \frac{Cash\ flow_t}{(1+\text{i})^t} - Investasi_{t=0} \quad \ldots\ldots (e)$$

Dengan,

NPV = Net Present Value
N = perioda
I = Discount Rate

Rumus (e) menunjukkan bahwa NPV tersebut memperhitungkan *dicount rate* sebagai faktor resiko atau ketidakepastian dari proyeksi *cash flows* sehingga proyeksi ash flows harus dilakukan penyesuain.

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 karena itu, tingkat suku bunga (i) dalam rumus-e menjadi nilai IRR yang dihitung berulang-ulang agar 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 *acual cost* didalam jaringan yang telah diletakkan pengangkat *intrussion Detection System (IDS)* dengan sebutan *Hummer*. Perangkat akan memberikan peringatan dini manakalah terdapat pola serangan yang dilakukan oleh *hacker*. Dari perhitungan teoritis, penentuan *tangible asset* seperti jaringan infrastrutur diukur dalam dollar dan *tangible asse*t 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 Expentancy* (ALE) [3]. Adapun rumusan ROI yang menggunakan IDS sebagai *security defence* adalah: *(ALE x IDS Efficiency) – Cost of IDS =ROSI* .....(f)

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 mengindentifikasikan juga bahwa bertambahnya investasi sistem keamanan informasi secara gradual tidak akan menaikan nilai ROSI terus-menerus. Hal ini ditunjukkan dari kurva *smokestack* (sumbu *survivability)* mengidentifikasikan bahwa perusahaan sangant rentan terhadap serangan keaamanan 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 investasi keamanan sistem. Pada titik tertentu, 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 harus bertambahnya investasi setelah *optimal seurity investement* terlewati *survivability* terhadap serangan akan bertamabah tetapi laju pertambahannya akan turun atau disebut sebagai *low of diminishing ROSI.*

Selanjutnya rumus-(f) mengalami penyederhanaan [9][13][14] menjadi: *(R-E) +T= ALE .....(*g)

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 Lost Expetancy (ALE):

R-(ALE) =ROSI .....(h)

Untuk menentukan *return on seurity investment* (ROSI), cukup mengurangkan kemungkinan kerugian dalam satu tahun (ALE)dari biaya tahunan untuk menperbaiki dari serangan(R). Untuk memperjelaskan hasil ru
mus (f), (g) dan (h) dapat diilustrasikan sebagai berikut:sebuah perusahaan jas pembiayaan keuangan memutuskan untuk menggunakan teknolgi *wireless remote access* untuk pengawaian ya 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 corporate information.*sebuah pengamanan dipergunakan dengan proteksi dilakukan dengan mekanisme security terpisah (*Ipsec tunnel)* yang bekerja 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 Trilyun, dan diperkirakan bahwa kerugian asset senilai 01% 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

= Rp. 6 Milyar

E = {ALE (Rp. 6 Miliyar) xEffktiifitas (0.85)} +

{Meningkatnya Produktifitasi (Rp 4 Miliyar) +

Penghematan biaya akses*Dial-up* (Rp.25.)}

E = Rp.11.6 Miliyar

ROSI = E (Rp.11.6 Miliyar) – Biaya Perangkat Pengaman(Rp.2.5M)

= Rp.9.1 Miliyar

Dari ilustrasi tersebut diatas maka implementasi *wireless remote access* dan investasi keamanan sistem informasi sebesar Rp. 2.5 M, akan memberikan ROSI senilai Rp 9.1 Miliyar. Dalam melakukan asumsi tersebut diatas, CISO harus mampu dan yakin dalam membuat perhitungan atau mengkuantifikasikan ancaman-ancaman kedalam angka. Termasuk didalamnya membuat statistik *security breach* yang terjadi didalam perusahan, menghitung probilytasnya dan effektifitas alat pengaman jika terjadi serangan sesungguhnya.

3.6.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 dikapilitasi agar dapat diperoleh manfaat yang besar. Pendekatan yang harus dilakukan untuk menghadapi ketidakpastian tersebut dapat menggunakan model *real options.* Model ini banyak dipergunakan untuk menilai *option* yang diperdagangkan dilembaga pasar modal. *Option* memiliki kesamaan dengan layanan yang dijual oleh lembaga asuransi untuk melindungi objek dari segala bentuk perusakan/ perubahan-nilai dalam jangka waktu tertentu, sehingga resiko yang dihadapi dipindahkan dipihak ketiga. Sebagai contoh asuransi rumah, asuransi jiwa dan asuransi kendaraan. Sedangkan objek 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 price)*denagn pembelian *option* dilakukan dimuka. Terdapat dua jenis *option*untuk menjual (*put options)*. *Call options* memberikan hak kepada pemilik untuk melakukan investasi dengan biaya dibayar dimuka *(excerccise 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 *exercise 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-*out souring*- 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 diatas 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 menggunakan metode *real options* yang dianggap sebagai teknik perhitungan keuangan mederen. Untuk teknik tradisional yang hanya mengenal keputusan untuk investasi atau tidak investasi, maka teknik tradisional ini menggunakan *discounted cash flows* untuk menghitung *present value*, seperti teknik NPV,IRR, ROI dan ROSI.

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

Perbedaan penting antara *tradisional valuation* dengan *real option* adalah faktor resiko atau ketidakpastian (*uncertainty)* yang termasuk dalam perhitungan. Dalam 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* Mempunyai nilai besar.Sedangkan dalam kondisi volatitas rendah,

NPV yang dihasilkan sangat kecil karena nilai *Option* Berharga kecil atau nol.

Sampai saat *Volatility* dianggap sebagai hal yang merugikan sehingga dalam perhitungan *discount rate* yang lebih tinggi (rumus-e) untuk teknik Tradisional. Akibat Proyek Investasi Keamanan sistem informasi dibentuk dari resiko yang sudah diprediksi diawal dan tidak akan dirubah selama proyek tersebut berlangsung.

Model *realoptions* berkaitan erat dengan teknik tradisional yang keduanya menggunakan. Sedangkan dalam teknik *discounted cash flows* dan fleksibilitas dari *uncertainty* diasumsikan tidak ada atau nol. Akibatnya model *real options* akan menghitung NPV yang telah diperluas (*extented 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 kkondisi untuk tetap melakukan investasi,(iii): kondisi option to shut down,dan(iv) kondisi option to switch. Akibatnya,*unertainty* dianggap Hal positif dan harus ditambahkan dalam traditional valuation (option value-C1 dari gambar 4-3), dan Uncertainty sebagai pegurang NPV dihilangkan (negatuf PV atau posisi garis A1-X1 dibawah sumbu A).

Adapun kondisi option to wait,option to shut down dan option to switch untuk investasi keamana sistem akan mempengaruhi pegerakan garis A-X(A adalah PV Proyrk dan X adalah excercise price) keatas dan kebawah sehingga volatility atas security breach akan memberi keuntungan terhadap perkembangan lingkungan yang ditunggu. Akibatnya, penantian pendapatan. Tetapi excercise real options lebih awal tentunya akan membrukan keuntungan yang lebih baik

IV. KESIMPULAN

Terjadi perubahan mendasar dalam menjalankan organisasi dari kegiatan tradisional ke organisasi yang terhubung dengan internet (*e-business)*,sehingga asset perusahaan yang berupa tersebut.pemeliharaan informasi tak terbatas terhadap gangguan yang dilakukan oleh pegawai perusahaan dan pengendalian arus data di dalam jaringan perusahaan. Pengamanan terhadap gangguan keamana sistem informasi harus secara proaktif dilakukan baik oleh CISO maupun kebijakan perusahaan,jika tidak mau kehilangan kapitalisasi pasar aktib pemberitaan publik.

Walaupun terdapat hubungan anatara strategi bisnis dan kondisi perusahaan dalam mengembangkan keamanan sistem informasi sebagai bagian dari investasi. Dampak ekonomi(Financial impact) perusahaan yang di gunakan sebagai kriteria pengambilan keputusan dalam pemanfaatan data internal dapat menggunakan teknik tradisional dan modren dalam memlakukan perhitungan invesitas kemanan 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 tinggu. Selain itu, fleksibilotas management untuk melakukan option to switch, option to stage investment dan options lainnya memberikan fleksibilitas bagi organisasi untuk menkaji posisi net beneft atas information security atau survivalibility-nya sudah mencapai titik optimun atau dengan bertambahnya security investment.

DAFTAR PUSTAKA

Computer Security Institute, “CSI/FBI Computes Crime and Scurity Survey 2000”, Eight Annual. http://www.gocsi.com

Dan Latimore, “Calculating Value During Uncertainty : Getting Real with Real Options”, IBM *Institute for Business Value*, 2002. http://www.ibm.com/service/strategy

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

Eva Kuiper, “The Really about Investing in Information Security”, *Security Investmen Justification, Hewlet-Packard,* Februari 2003. http://www.hp.com

Hary Sucipto, “Model Bisnis WLAN di Indonesia*”, Makalah Tugas Jaringan Nirkabel dan Bergerak* (E1-7021), MTI-ITB, Desember 2003.

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

Stephen A. Ross, W.W Westerfield dan J.F. Jaffe, “Value and Capital Budgeting”, *Corporate Finance*, Edisi 3, Irwin Publishing,1998

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

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

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