
TUGAS UJIAN AKHIR
KAJIAN BISNIS & EKONOMI UNTUK IMPLEMENTASI
KEAMANAN SISTEM INFORMASI

EC-7010
KEAMANAN SISTEM LANJUT



Oleh :

Hary Sucipto

NIM : 23202064

Program Pasca Sarjana Option Teknologi Informasi
Departemen Teknik Elektro – Fakultas Teknologi Industri
Institut Teknologi Bandung
Januari 2004

DAFTAR ISI

DAFTAR ISI	1
ABSTRAK	2
1. PENDAHULUAN	3
1.1. Tujuan Laporan	3
1.2. Kerangka Pembahasan	3
2. ASPEK-ASPEK EKONOMI DARI KEAMANAN SISTEM INFORMASI	5
2.1. Frekuensi Pelanggaran Keamanan Informasi	6
2.2. Kerugian Atas Pelanggaran Keamanan Sistem Informasi	7
2.3. Proses Investasi Keamanan Sistem Informasi	9
2.4. Reaksi Portfolio Investor Terhadap <i>Security Breach</i>	10
2.4.1. Metodologi <i>Event Study</i>	10
2.2.2. Hasil <i>Event Study</i>	12
3. MODEL EKONOMI & BISNIS UNTUK MENGENAL IMPLEMENTASI KEAMANAN SISTEM INFORMASI	14
3.1. <i>Marginal Analysis</i>	16
3.2. <i>Return On Investment (ROI)</i>	17
3.3. Konsep <i>Value of Money</i>	18
3.3.1. <i>Present Value</i>	18
3.3.2. <i>Internal Rate of Return (IRR)</i>	19
3.4. <i>Return On Security Investment (ROSI)</i>	19
3.5. <i>Real Options Model</i>	22
4. EVALUASI MODEL EKONOMI	25
5. KESIMPULAN	28
REFERENSI	29

Abstrak

Melakukan kajian ekonomi dan bisnis untuk implementasi information security sudah harus dilaksanakan. Perubahan perlakuan implementasi information security dari cost budgeting ke investment budgeting ini, maka diperlukan metoda perhitungan yang tepat. Hal ini dilaksanakan, mengingat semua capital dan operational expenditures harus memiliki financial impact yang besar bagi organisasi, tak terkecuali di bidang information security.

Model Real Options yang merepresentasikan teknik perhitungan keuangan modern, mulai menggeser teknik perhitungan tradisional seperti ROI, ROSI dan NPV. Real options yang dianggap sebagai extended NPV dapat mengakomodasi fleksibilitas management dalam mengevaluasi proyek investasi keamanan sistem informasi terhadap gejolak perubahan lingkungan yang besar. Fleksibilitas tersebut dapat digunakan dalam mengukur kemampuan optimal dari information security yang selalu berubah seiring perubahan volatility dari security breach.

BAGIAN I

PENDAHULUAN

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*.

1.1. TUJUAN LAPORAN

Penyusunan laporan ini bertujuan untuk [1]: mengetahui kecenderungan korporasi dalam memahami pentingnya *information security* untuk kelangsungan usaha jangka panjang, [2]: Membahas secara detil suatu kajian bisnis dan ekonomis dalam mengimplementasikan *information security* di perusahaan, sehingga manajemen puncak sebagai pengambil keputusan dapat memahami *cost-benefits* dan model ekonomi dalam memperoleh sumber daya tersebut.

1.2. KERANGKA PEMBAHASAN

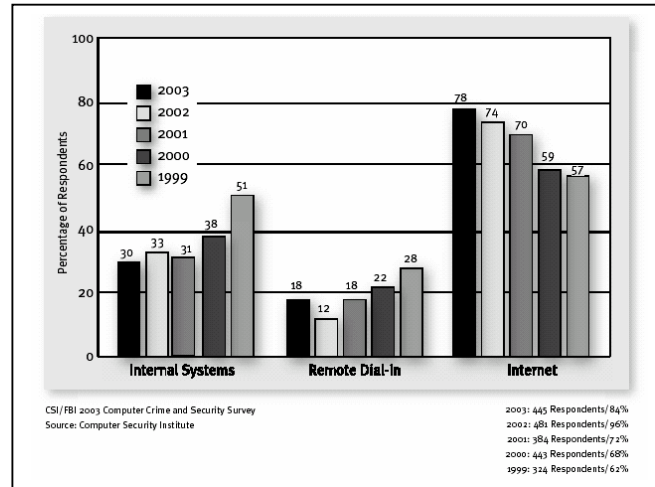
Manfaat yang diperoleh dari implementasi keamanan sistem informasi sangat tergantung dari kondisi lingkungan. Selain itu, kemampuan suatu organisasi dalam memberdayakan kondisi lingkungan akan dapat menciptakan manfaat yang optimal. Kemampuan tersebut sangat bervariasi dari satu organisasi dengan organisasi lainnya, sehingga evaluasi ekonomis dan bisnis atas sifat teknis dari keamanan sistem informasi sangat sulit dilakukan.

Untuk memahami permasalahan yang dihadapi oleh organisasi dalam menginvestasikan *information security*, maka kerangka pembahasan dimulai 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.

BAGIAN II

ASPEK-ASPEK EKONOMI DARI KEAMANAN SISTEM INFORMASI

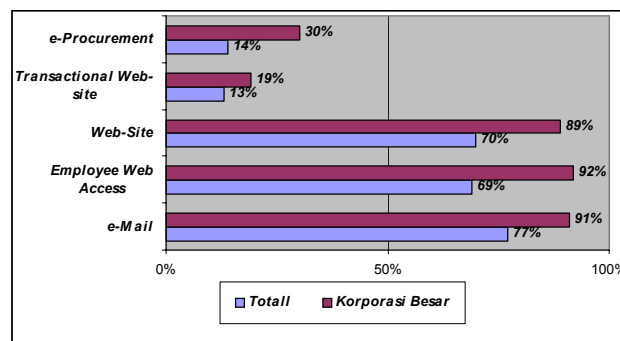
Dari survey yang dilakukan oleh *PriceWaterHouse-Coopers* pada tahun 2002 menunjukkan bahwa lingkungan bisnis yang terjadi di Inggris dan US telah terjadi perubahan, yakni dengan memberdayakan kemampuan internet untuk melakukan aktifitas *e-business*[1]. Pemanfaatan internet ini memberi dampak langsung terhadap keamanan sistem informasi dan menjadikan internet sebagai pintu gerbang serangan ke sistem informasi suatu organisasi [2].



Gambar 2-1 : Koneksi Internet sebagai Sumber Serangan Sistem Informasi [2]

Hasil survey dari tahun 1999 sampai 2003 yang dilakukan CSI/ FBI terhadap responden 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 survey di perusahaan Inggris, dimana internet dipergunakan untuk

mengirim e-mail. Tercatat 77% total perusahaan dan 91% korporasi besar menggunakan e-mail sebagai bentuk korespondensi antar pegawai [1].



Gambar 2-2: Implementasi e-Business di Inggris [1]

Selain itu diketahui pula bahwa 69% total perusahaan dan 92% perusahaan besar yang disurvei memberikan kesempatan kepada pegawainya untuk menggunakan akses *web* (gambar 2-2). Yang menarik dari hasil tersebut menunjukkan pula, hanya 13% perusahaan yang menerima transaksi perdagangan dengan meng-

gunakan *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 (B2B), 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 investasi yang berkaitan dengan keamanan sistem informasi [3], dan (iv) Reaksi portfolio investor terhadap pelanggaran keamanan sistem informasi yang diumumkan untuk publik[4,5,6].

2.1. 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* (Gambar2-3) [7]. *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 worms			●		
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 "hactivism" or cyber protest		●			
Cyber-terrorism—foreign-based		●			
Cyber-terrorism—domestic-based		●			
Non-nuclear terrorist attack		●			
Cyber War		●			
Foreign government espionage		●			

Gambar-2-3 : Intensitas Ancaman dalam Keamanan Sistem Informasi untuk Tahun Mendatang [7]

Sedangkan intensitas ancaman urutan kedua diakibatkan oleh status kepegawaian seseorang, dan diikuti dengan intensitas urutan ketiga yakni *distributed Denial of Services attack (DDoS)* (gambar 2-3).

Hasil temuan tersebut diatas sangat konsisten dengan survey yang dilakukan di Inggris tahun 2002 [1] dan di USA 2003 [2], 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[1]. Sebagai contohnya, di tahun 1998 pelanggaran telah dialami oleh 18% responden. Selanjut-nya terjadi peningkatan lebih dari dua kali di tahun 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
<small>2003: 356 Respondents/67%, 2002: 322 Respondents/64%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%</small>						
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
<small>2003: 336 Respondents/63%, 2002: 301 Respondents/60%, 2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%</small>						
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
<small>2003: 328 Respondents/62%, 2002: 289 Respondents/57%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%</small>						

Gambar 2-4 : Frekuensi Kejadian Pelanggaran Sistem Keamanan [2]

Dari kejadian-kejadian pelanggaran sistem keamanan informasi di USA dilaporkan bahwa frekuensi pelanggaran untuk kejadian kurang dari 6 kali dalam satu tahun lebih banyak dihadapi oleh setiap perusahaan (gambar 2-4). Yang menarik dari hasil tersebut adalah tingginya persentase organisasi yang tidak mengetahui frekuensi kejadian pelanggaran keamanan sistem informasinya, baik yang berasal dari luar dan dari dalam organisasi tersebut.

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

2.2. KERUGIAN ATAS PELANGGARAN KEAMANAN SISTEM INFORMASI

Di Inggris, hampir dua pertiga kejadian pelanggaran menimbulkan kerugian kurang dari USD 15.000 [1]. 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.

How Money Was Lost																	
	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses				
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03	
Theft of proprietary info.	\$1K	\$100	\$1K	\$2K	\$25M	\$50M	\$50M	\$35M	\$3,032,818	\$4,447,900	\$6,571,000	\$2,699,842	\$66,708,000	\$151,230,100	\$170,827,000	70,195,900	
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500	
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,000	76,000	
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400	
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200	
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400	
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300	
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340	
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	300,000	31,254	22,554,500	6,064,000	4,503,000	406,300	
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,000	701,500	
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000	
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500	
												Total Annual Losses		265,337,990	377,828,700	455,848,000	201,797,340

Gambar 2-5 : Kerugian untuk Setiap Jenis Pelanggaran Keamanan Sistem [2]

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 2-5, *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.

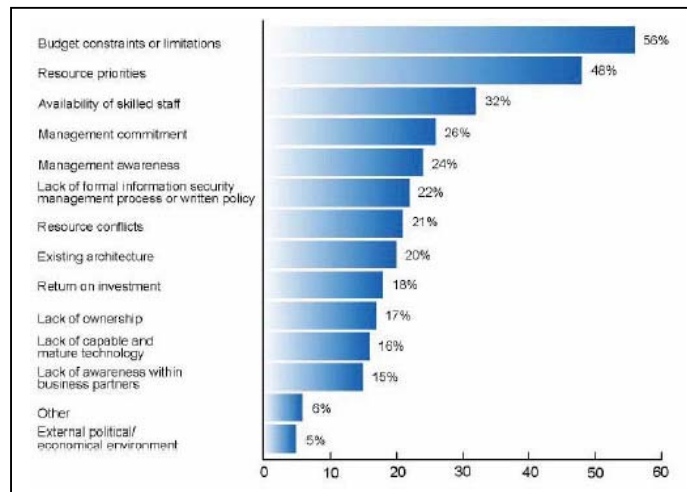
Gangguan keamanan sistem yang diakibatkan oleh infeksi virus hanya menempati urutan ketiga dari total kerugian tahunan yakni sebesar US\$ 27 Juta. Nilai kerugian tersebut tidak sebanding dengan intensitas ancaman yang diprediksi di 12 bulan kedepan yang menduduki prioritas tertinggi.

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 perusahaan masing-masing[7]. Sedangkan 34% organisasi tidak menggunakan jasa asuransi untuk mengatasinya. Sisanya (33%) masih tetap menjadi persoalan di dalam 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 pengelola perusahaan saja, tetapi juga oleh penyedia jasa asuransi.

2.3. PROSES INVESTASI KEAMANAN SISTEM INFORMASI

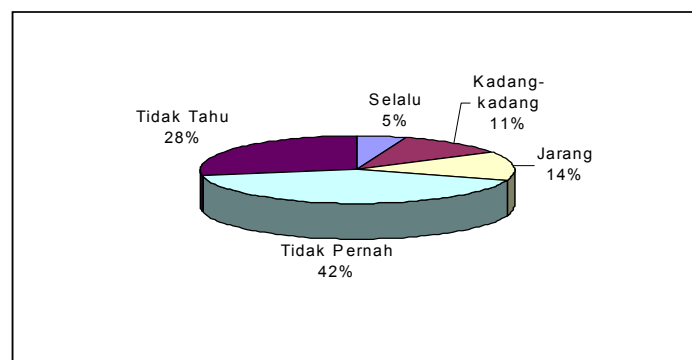
Biaya yang dikeluarkan untuk membangun keamanan sistem informasi sampai saat ini masih dianggap sebagai pengeluaran rutin (*expenses*) sehingga pengeluaran biaya tersebut tidak menjadi prioritas utama dan tidak diperlakukan sebagai investasi.



Gambar 2-6: Hambatan Implementasi Keamanan Sistem [7]

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 mengimplementasikannya, dan pengembangan tersebut tidak dianggap sebagai prioritas utama (48%) jika dibandingkan dengan sumber daya lainnya yang dimiliki oleh perusahaan [7].

Perlakuan implementasi keamanan sistem sebagai pengeluaran rutin (*expenses*) ini, maka 59% organisasi global [7] dan 84% perusahaan Inggris [1] tidak pernah, jarang dan tidak tahu menggunakan perhitungan *Return on Investment (ROI)* untuk biaya pengeluaran keamanan sistem informasi.



Gambar 2-7 : Penggunaan ROI untuk *Security Expenditure* di Inggris[1]

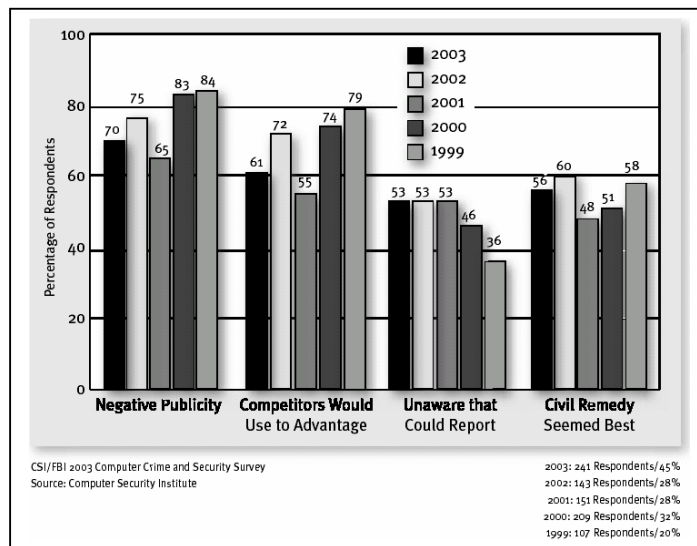
Terdapat beberapa alasan untuk tidak menggunakan perhitungan ROI untuk pengeluaran biaya keamanan sistem, yakni (i): manfaat yang ditimbulkan dari pemanfaatan keamanan sistem bersifat intangible atau sukar diukur seperti hilangnya waktu tunggu pegawai pada saat

terjadi gangguan; (ii): banyak profesional keamanan sistem memiliki latar belakang pendidikan teknis sehingga kemampuan untuk mengembangkan *business case* sangat terbatas [1]; (iii): komitmen manajemen puncak sangat rendah terhadap keamanan

sistem informasi dikala mereka belum menghadapi kejadian berat yang mempengaruhi kinerja suatu perusahaan; (iv) cara penghitungan ROI hanya dilakukan untuk melakukan kajian investasi yang memiliki nilai yang cukup besar dan berkaitan langsung terhadap pendapatan/ *revenue* suatu perusahaan, sehingga untuk semua jenis *expenses* tidak diperlukan perhitungan tersebut.

2.4. REAKSI PORTFOLIO INVESTOR TERHADAP *SECURITY BREACHING*

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



Gambar 2-8 : Alasan Tidak Melaporkan *Security Breaching* bagi Organisasi di USA [2]

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

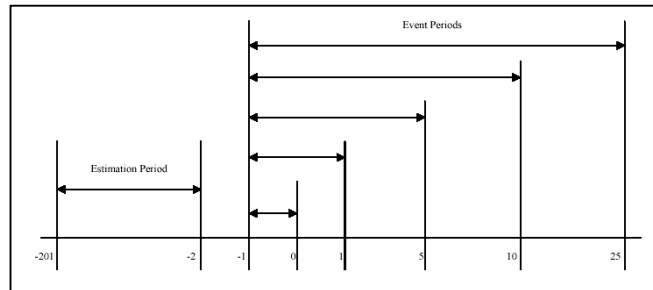
Pemberitaan negatif tentang *security breach* bagi perusahaan publik yang tercatat di bursa saham diperkirakan akan mempengaruhi performansi nilai saham untuk jangka pendek dan jangka panjang. Dampak tersebut dapat dipahami dengan menggunakan metoda analisa *event study*.

2.4.1. Metodologi *Event Study*

Untuk pasar modal yang memiliki kondisi *Efficient Market Hypotheses (EMH)*, segala bentuk informasi baru yang masuk ke pasar modal dan berkaitan dengan pemberitaan emiten (*listed company*), maka *portfolio investor* akan melakukan

penyesuaian harga saham dengan cepat [8]. Penyesuaian harga saham tersebut mencerminkan pengaruh informasi baru yang berkaitan dengan *security breach* termasuk didalamnya resiko-resiko yang mungkin akan timbul seperti *potential financial losses*.

Pengkajian terhadap (i): pergerakan harga saham di saat-saat pemberitaan *security breach* dan (ii): waktu terjadinya penyesuaian harga, akan memberikan indikasi kepada publik apakah pemberitaan tersebut disebarakan secara terbatas atau luas. Jika



Gambar 2-9: Periode Event Study [5]

harga saham perusahaan publik yang mengalami *security breach* terjadi pergerakan besar, yakni satu hari (H-1) sebelum diumumkan kepada publik (H), maka pergerakan besar harga saham untuk periode *event* $\{-1,0\}$ 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 diumumkan kepada publik, maka pergerakan-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 announcement* tidak akan memiliki makna, jika *return* dari agregat semua harga saham mengikuti pola yang sama.

Abnormal rate of return dapat diformulasikan sebagai berikut,

$$AR_{it} = R_{it} - R_{mt} \dots\dots\dots(a)$$

Dimana, AR_{it} = *Abnormal Rate of Return* untuk Saham *i* selama kurun waktu *t*
 R_{it} = *Rate of Return* untuk Saham *i* selama kurun waktu *t*
 R_{mt} = *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 Stock Exchange*) mengalami kenaikan sebesar 2%. Dari informasi tersebut dapat dikatakan bahwa perubahan abnormal harga (*abnormal price change*) untuk periode *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*, dimungkin pula untuk mengkaji dampak keseluruhan terhadap pengumuman tersebut disekitar *event*, sehingga penghitungan *abnormal rate of return* disekitar *event* akan menghasilkan *cumulative abnormal return* (CAR).

$$CAR_i = \sum_{t=1}^n AR_{it} \quad \dots\dots\dots(b)$$

Dari uraian diatas diperoleh dua pendekatan untuk mengamati perubahan harga abnormal disekitar saat-saat pengumuman *security breach* untuk melihat penyesuaian harga, atau mengamati *abnormal rate of return* sesaat setelah diumumkan *security breach* untuk melihat kemungkinan investor memperoleh *above average rate of return* dalam kondisi *Semistrong Efficient Market Hypotheses* [8].

2.4.2. Hasil *Event Study*

Untuk mengetahui dampak yang dihadapi oleh emiten yang mengalami *security breach*, beberapa *event study* telah dilakukan meliputi *corporate information security breach*[4], *Denial-of-Service*[5] dan *internet security breach* [6].

Jenis *Internet security breach* yang banyak dilakukan adalah serangan *denial of services* (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 ke server perusahaan dan biasanya merupakan *web server* dan penyerang menjalankan program *Ping* berulang kali 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 dilakukan terhadap perusahaan-perusahaan publik yang tercatat di New York Stock Exchange (NYSE) dan NASDAQ *stock exchange*. *Event study* yang dilakukan terhadap 23 perusahaan publik untuk perioda *event* $\{-1,0\}$, $\{-1,+1\}$, $\{-1,+5\}$, $\{-1,+10\}$ dan $\{-1,+25\}$ menunjukkan bahwa 48% publikasi yang berisi berita tentang serangan DOS memberikan nilai *negative abnormal rate of return* (AR) [5].

Selanjutnya, 23 perusahaan publik tersebut dikelompokkan ke perusahaan yang berbasis internet untuk bisnis intinya, dan ke perusahaan yang bisnis intinya tidak berkaitan langsung dengan internet. *Event study* terhadap kedua kolompok 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* [5]. Perubahan harga saham tersebut diakibatkan oleh ekspektasi investor terhadap nilai ekonomi perusahaan karena berkurangnya *cash flow* perusahaan yang dialokasikan untuk 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 investasi harus dilakukan, dan perlakuan keamanan sistem informasi sebagai *expenses* harus ditinggalkan.

Sedangkan *event study* terhadap perusahaan publik yang menghadapi *corporate information security breach* hanya membatasi permasalahannya pada dampak akses *illegal* terhadap informasi rahasia perusahaan (*unauthorized access to confidential information*), dan dampak akses *illegal* terhadap informasi dengan klasifikasi biasa (*unauthorized access 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 biasa adalah (i): *virus*, (ii): *Denial of Services* dan (iii): gangguan terhadap *website* perusahaan.

Even study dilakukan terhadap 43 perusahaan publik yang mengalami *corporate information security breach* sejak Januari 1995 sampai Desember 2000 dengan perbandingan 11 *sample* masuk kategori *unathorized access confidential information* dan 32 *sample* sebagai kategori *unauthorized access non-confidential information*. *Public announcement* untuk setiap perusahaan publik selanjutnya dianalisa dampaknya disekitar perioda *event* selama tiga hari atau $\{-1,+1\}$.

Hasil pengamatan yang dilakukan oleh Champbel, Gordon dan Zhou menunjukkan bahwa perusahaan publik yang menghadapi *unauthorized access non-confidential information* menghasilkan negatif CAR, yakni penurunan harga saham sebesar 0.7% setelah kejadian tersebut dipublikasikan. Disamping itu, perusahaan yang mengalami penurunan harga saham karena pelanggaran diatas sebesar dialami oleh 40.63% sampel.

Sebaliknya, penurunan harga sahan semakin besar (minus 5.5 %) manakala kejadian yang berkaitan dengan *unauthorized access confidential information* dipublikasikan [4]. 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 berkaitan 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 *competitive advantage* rivalnya baik berupa kepercayaan yang telah dibangun dengan *customer* maupun *partner* bisnisnya. Hal ini konsisten dengan hasil survey (lihat gambar 2-8), 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 [6]. Lingkup *internet security breach* meliputi *Denial of Service*, *IT failure* dan *security incident* lainnya.

Dari 66 perusahaan publik yang diuji untuk periode *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 periode event $\{-2,+2\}$. Penurunan harga saham tersebut setara dengan kerugian kapitalisasi pasar (*market capitalization*) sekitar US\$ 1.65 milyar untuk satu kali peristiwa[6].

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

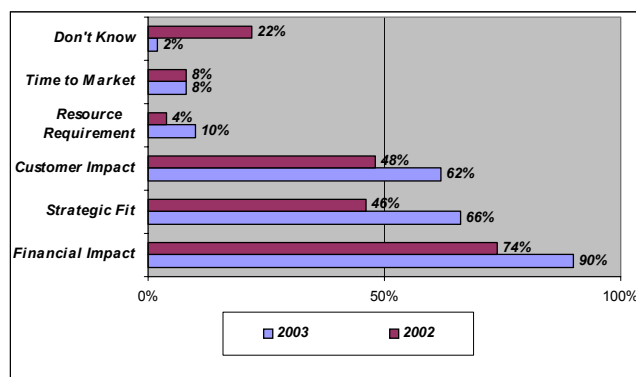
Dengan kata lain, kenaikan kapitasi pasar bagi perusahaan yang mengimplementasikan keamanan sistem baru, mengindikasikan reaksi penyesuaian harga saham yang dilakukan oleh *portfolio investor* atas sinyal yang dikeluarkan oleh emiten. Sinyal tersebut dianggap bahwa perusahaan mempunyai komitmen jelas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

Sebaliknya, emiten yang lalai dalam melakukan *continous improvement* terhadap keamanan sistem informasi di perusahaan 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 kerugian yang diakibatkan oleh *average cost* yang dikeluarkan untuk memperbaiki sistem informasi untuk setiap kejadian dari masing-masing jenis *security breach* (lihat gambar 2-5).

BAGIAN III

MODEL EKONOMI DAN BISNIS UNTUK MENGENAL IMPLEMENTASI *INFOSEC*

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.



Gambar 3-1 : Kriteria Pengambilan Keputusan untuk Pendanaan Internal Perusahaan [9]

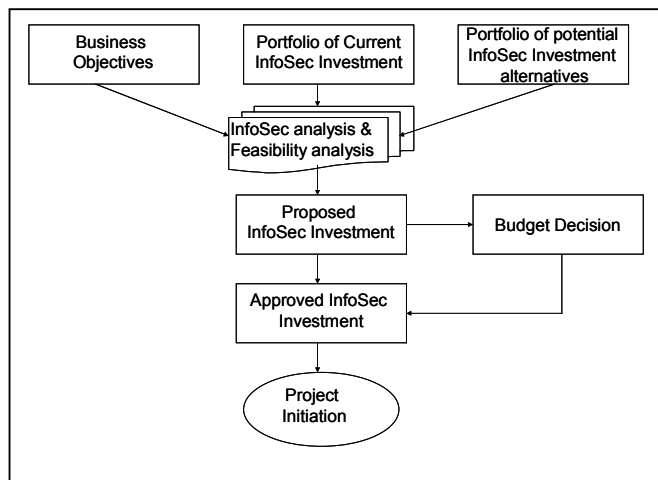
Dilain pihak, pimpinan puncak dan manajemen madya suatu perusahaan dalam proses pengambilan keputusan selalu mempertimbangkan dampak finansialnya untuk setiap penggunaan dana internal perusahaan [9] (gambar 3-1). Selain dampak finansial sebagai kriteria utama, kriteria berikutnya adalah mempertimbangkan pula kesesuaian (*strategic fit*) antara *resources* 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 memenuhi sasaran bisnis (*business objectives*) jangka pendek dan jangka panjang dari organisasi.



Gambar 3-2 : Proses Portfolio Manajemen untuk *InfoSec* (modifikasi dari [10])

Managemen portfolio keamanan sistem informasi memberikan pendekatan yang terpadu dalam melakukan identifikasi, pemilihan, kontrol, evaluasi dan management investasi keamanan sistem (gambar 3-2) [10].

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.

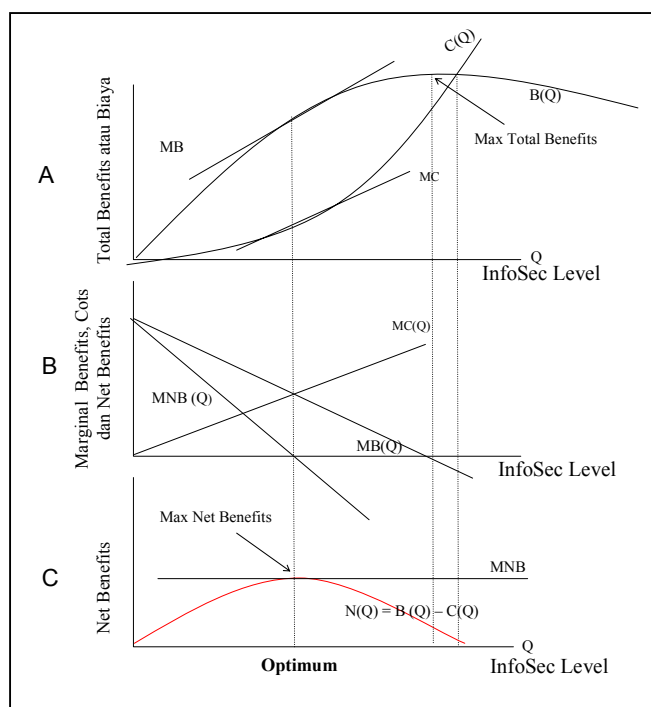
3.1. MARGINAL ANALYSIS

Marginal analisis merupakan salah satu cara pengambilan keputusan bagi CISO dengan membandingkan antara marginal manfaat yang dihasilkan dengan marginal biaya. Sebagai contohnya, Gambar 3-3A menunjukkan total manfaat yang dihasilkan dari setiap unit variabel keamanan sistem informasi (*InfoSec Level*) yang dikelola oleh CISO [3]. Secara umum dapat dikatakan pula bahwa $B_{benefits}(Q)$ dapat diperoleh dari level keamanan sistem informasi yang diharapkan, dan sebanding dengan $C_{osts}(Q)$ 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 (gambar 3-3C).

$$N(Q) = B(Q) - C(Q) \quad \dots\dots(c)$$

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



Gambar 3-3 : Kurva Manfaat dan Biaya untuk Keamanan Sistem Informasi
(Sumber: grafik-A: [3]; grafik-B & C: [11])

Untuk memberikan betapa pentingnya *marginal analysis* dalam memaksimalkan *net benefit* maka hubungan antara *marginal benefit*, *marginal costs* dan *marginal net benefit* dapat diilustrasikan di gambar 3-3B.

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*.

$$MNB(Q) = MB(Q) - MC(Q) \dots\dots(d)$$

Pada kondisi level *InfoSec* optimal, kurva *marginal benefit* akan berpotongan dengan kurva *marginal cost* sehingga *marginal net benefit*nya 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 *preliminary 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 dikeluarkan 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)* [12].

3.3.1. 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[12].

$$NPV = \sum_{t=1}^n \frac{CashFlow_t}{(1+i)^t} - Investasi_{t=0} \dots\dots(e)$$

dengan, NPV = Net Present Value n = Periode
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.

3.3.2. 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 $NPV=0$ [12].

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 INVESTMENT (ROSI)

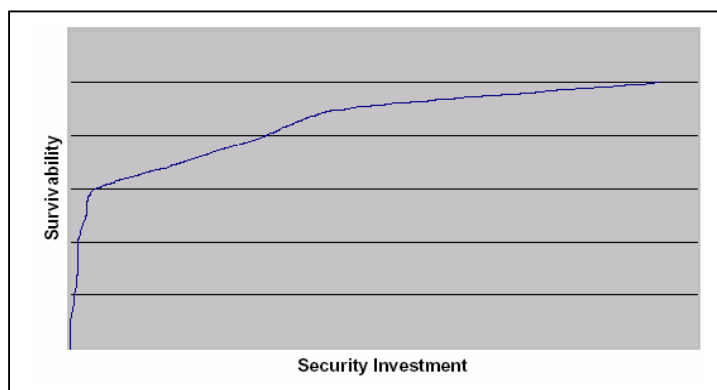
Di tahun 2000 dan 2001, beberapa peneliti di Universitas Idaho-USA telah membuat rumusan untuk menghitung *Return on Investment* bagi keamanan sistem informasi. Rumusan tersebut dikenal sebagai *Return on Security Investment (ROSI)*[13].

Para peneliti awalnya ingin menguji perhitungan teoritis dengan *actual cost* di dalam jaringan yang telah diletakkan pengangkat *Intrusion 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 infrastruktur 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) [13]. Adapun rumusan ROI yang menggunakan IDS sebagai *security defence* adalah :

$$(ALE \times IDS \text{ Efficiency}) - \text{Cost of IDS} = \text{ROSI} \dots\dots(f)$$

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 [9][13].



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* (gambar 3-4).

Gambar 3-4 : Kurva *Smokestack* [12]

Nilai terendah dari sumbu tegak dari kurva *smokestack* (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.

Gambar 3-4 menjelaskan kondisi *survivability* yang mempunyai laju kenaikan lebih cepat dibandingkan laju kenaikan nilai 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 terus bertambahnya investasi setelah *optimal security investment* terlewati, *survivability* terhadap serangan akan bertambah tetapi laju pertumbuhannya akan turun atau disebut sebagai *law of diminishing ROSI*.

Selanjutnya rumus-(f) mengalami penyederhaaan [9][13][14] menjadi :

$$(R - E) + T = ALE \dots\dots(g)$$

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
 serangan

dari persamaan (g) akan diperoleh Annual Loss Expetancy (ALE) [9][13][14]

$$R - (ALE) = ROSI \dots\dots(h)$$

Untuk menentukan *return on security investment* (ROSI), cukup mengurangi kemungkinan kerugian dalam satu tahun (ALE) dari biaya tahunan untuk memperbaiki dari serangan (R).

Untuk memperjelas hasil rumus (f), (g) dan (h) dapat diilustrasikan 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 [15]. 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 :

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

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 Milyar.

Dalam melakukan asumsi tersebut diatas, CISO harus mampu dan yakin dalam membuat perhitungan atau mengkuantifikasi ancaman-ancaman kedalam angka. Termasuk didalamnya membuat statistik *security breach* yang terjadi di dalam perusahaan, menghitung probabilitasnya dan efektifitas alat pengaman jika terjadi serangan sesungguhnya[16].

3.5. REAL OPTION MODEL

Perkembangan dari *security breach* menjadi semakin kompleks dan sulit untuk diprediksi kapan akan terjadi. Akibatnya CISO menghadapi ketidakpastian (*uncerainty*) 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[17]. *Option* memiliki kesamaan dengan layanan yang dijual oleh lembaga asuransi untuk melindungi obyek dari segala bentuk kerusakan / 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.

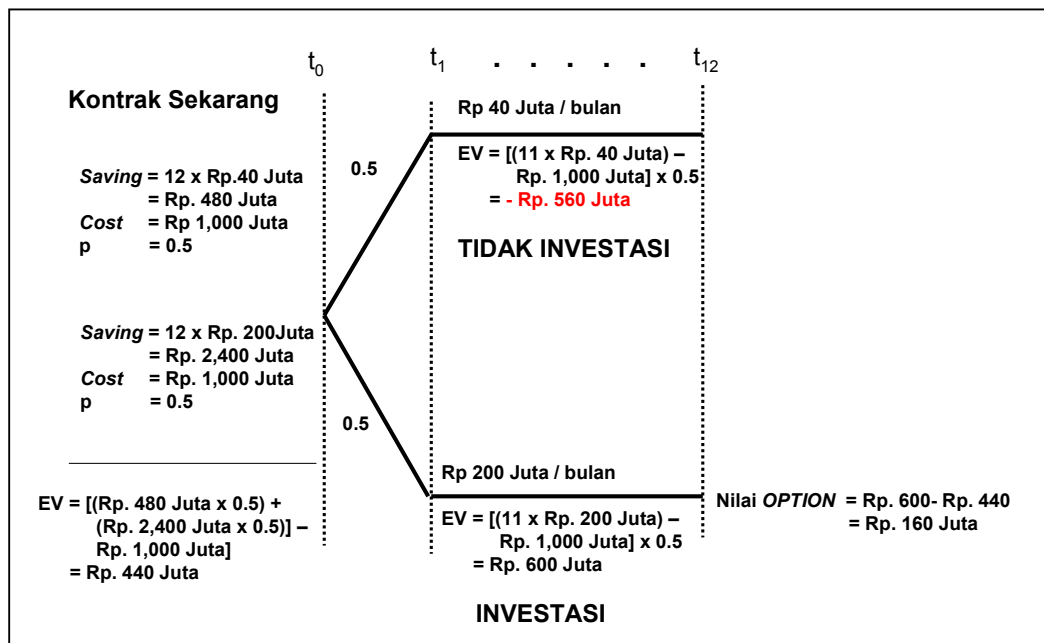
Options memberikan hak kepada pemilik *option* untuk melakukan sesuatu, dan pemilik berhak untuk menjualnya (*exercise right*) dengan pembelian *options* dilakukan dimuka. Terdapat dua jenis *option*, yakni *option* untuk membeli (*call options*) dan *option* untuk menjual (*put options*).

Call options memberikan hak kepada pemilik untuk melakukan investasi dengan biaya dibayar dimuka (*exercise 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 [11][17][18][19].

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 *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 diatas maka *option valuation* dapat dihitung dengan menggunakan model *binomial* sederhana [20], selain model *Black-Scholes* yang memiliki kompleksitas tinggi [17] tidak dibahas dalam makalah ini.



Gambar 3-5 : Model *Real Put Options* (Modifikasi dari [20])

Gambar 3-5 menjelaskan keputusan dalam pemanfaatan anggaran Rp. 1 Milyar yang diperlakukan sebagai *put option*. Jika perusahaan memberikan kontrak memperbaiki keamanan sistem ke pihak ketiga, anggaran tersebut harus dikeluarkan, dan penghematan biaya operasional hanya diperoleh sebesar Rp. 480 Juta untuk 12 bulan. Penghematan ini sangat kecil dibandingkan dengan biaya yang dikeluarkan, tetapi peluang yang terjadi sebesar 50% ($p=0.5$).

Dengan perkiraan intensitas *security breach* setahun kedepan yang tinggi seperti ditunjukkan dalam gambar 2-3 maka perusahaan dapat melakukan penghematan biaya operasional setahun sebesar Rp. 2.4 Milyar untuk memperbaiki sistem informasi perusahaan, jika perbaikan keamanan sistem dikontrakkan ke pihak ketiga. Kondisi ini memiliki probabilitas sebesar 50% juga ($p=0.5$).

Dari probabilitas kedua kondisi tersebut, *expected value* yang diperoleh sebesar Rp. 440 Juta untuk penandatangan kontrak saat sekarang (t_0). Pelaksanaan implementasi tersebut dapat tetap terus dilakukan atau ditunda satu bulan di t_1 . Jika mengalami penundaan satu bulan untuk memastikan kondisi *uncertainty* lebih baik, maka *put option* jatuh pada kondisi sebelah atas/ normal, maka *Expected Value* (EV) senilai (-Rp.560) Juta mempunyai *option value* sebesar Rp.0. Manakala *put option* jatuh pada kondisi *security breach* dengan intensitas tinggi, maka *Expected Value* senilai Rp. 600 Juta mempunyai *option value* sebesar Rp. 160 Juta.

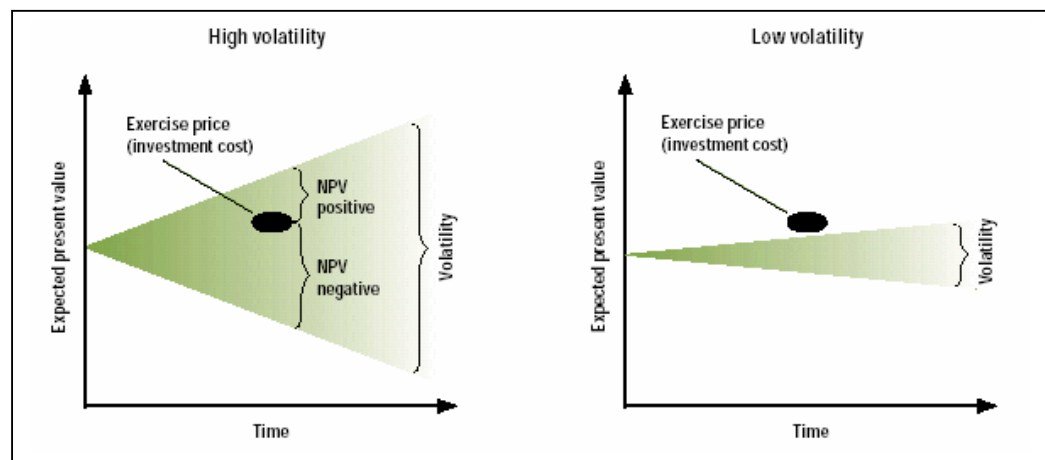
Dari gambaran tersebut, CISO mempunyai kewajiban untuk memperoleh manfaat yang besar dalam kondisi lingkungan yang tidak pasti (*uncertainty*) dengan mempergunakan model *real options*. Model ini memberikan kesempatan kepada CISO untuk terus melanjutkan, menunda atau membatalkan investasi dan kontrak perbaikan keamanan sistem. Salah satu dari ketiga pilihan tersebut harus diambil ketika berjalannya waktu ditemukan data tambahan, sehingga merubah hasil keputusan awal.

BAGIAN IV

EVALUASI MODEL EKONOMI

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 metoda *real options* 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 flows* 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 sebelumnya *economic life* untuk ilustrasi ROSI hanya diperhitungkan satu tahun.

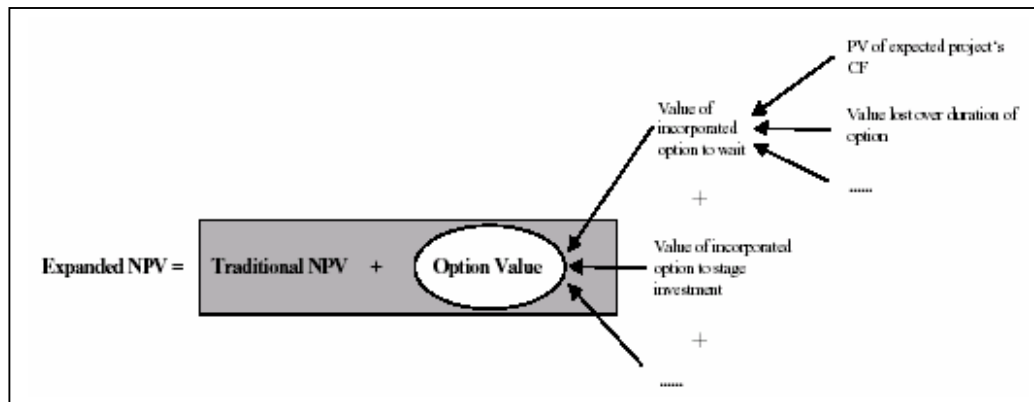
Perbedaan penting antara *tradisional valuation* dengan *real option* adalah faktor resiko atau ketidakpastian (*uncertainty*) yang masuk dalam perhitungan. Untuk lingkungan yang memiliki *uncertainty* sangat tinggi, model *real option* menjadi lebih bernilai sehingga *option value* menjadi lebih besar.



Gambar 4-1 : Gejala Perubahan sebanding dengan nilai real options [18]

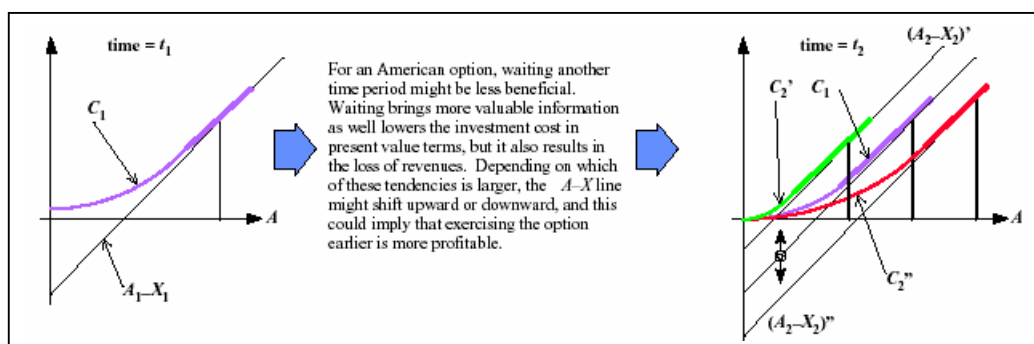
Present value suatu investasi dapat dihitung dengan tepat manakala investasi telah dilaksanakan seiring berjalannya waktu sehingga ketidakpastian (*uncertainty*) telah diketahui dengan pasti[18]. Dari gambar 4-1 terlihat bahwa untuk lingkungan dengan gejala perubahan sangat tinggi (*high volatile*), 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 [21]. Akibatnya proyek investasi keamanan sistem informasi dibentuk dari resiko yang sudah diprediksi diawal dan tidak akan dirubah selama proyek tersebut berlangsung.



Gambar 4-2 : Expanded NPV [21]

Model *real options* berkaitan erat dengan teknik tradisional yang keduanya menggunakan pendekatan *discounted cash flows* dan fleksibilitas dari *uncertainty*. Sedangkan dalam teknik tradisional, fleksibilitas 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* [21], seperti ditunjukkan dalam gambar 4-2. 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*.



Gambar 4-3 : Perbandingan real options dengan teknik tradisional [19]

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 *exercise price*) keatas dan kebawah sehingga *volatility* atas *security breach* akan memberi keuntungan terhadap perkembangan lingkungan yang ditunggu. Akibatnya, penantian tersebut akan menurunkan biaya investasi untuk PV, dan hilangnya pendapatan. Tetapi *exercise real options* lebih awal tentunya akan memberikan keuntungan yang lebih baik.

BAGIAN V

KESIMPULAN

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*.

REFERENSI

- [1] PriceWaterHouse-Coopers, “*Information Security Breaches Survey 2002 : Technical Report*”, April 2002. <http://www.security-survey.gov.uk/>
- [2] Computer Security Institute, “*CSI/FBI Computer Crime and Security Survey 2003*”, Eight Annual. <http://www.gocsi.com/>
- [3] L.A. Gordon dan M.P. Loeb, “*Economics Aspect of Information Security*”, Rainbow Technologies, v.2.1, Agustus 2001.
- [4] 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.
- [5] A. Hovav dan J. D’Arcy, “*The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms*”, MIS Department, Fox School of Business, Temple University, Maret 2003.
- [6] 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.
- [7] Ernst & Young, “*Global Information Security Survey 2003*”. <http://www.ey.com/global>
- [8] Frank K. Reilly, “*Efficient Capital Markets*”, *Investment Analysis and Portfolio Management*, Edisi ke-3, The Dryden Press International Edition, 1989.
- [9] Eva Kuiper, “*The Reality about Investing in Information Security*”, *Security Investment Justification*, Hewlet-Packard, Pebruari 2003. <http://www.hp.com/>
- [10] Washington State Department of Information Services, “*Information Technology Planning and Assessment Guidelines*”, Mei 1999. <http://www.wa.gov/dis/portfolio>
- [11] Michael R. Baye, “*Managerial Economics & Business Strategy*”, McGraw-Hill Higher Education, Edisi-3, 2000.
- [12] Stephen A. Ross, W.W. Westerfield dan J.F. Jaffee, “*Value and Capital Budgeting*”, *Corporate Finance*, Edisi-3, Irwin Publishing, 1988.
- [13] Steve Foster dan Bob Pacl, “*Analysis of Return on Investment for Information Security*”, A White Paper, Getronics. <http://www.getronics.com/us>
- [14] Q1Labs, “*Illegal Peer-to-Peer File Sharing: Are You Protected*”, *Q1 Labs White Paper*, Maret 2003. <http://www.q1labs.com/>
- [15] Hary Sucipto, “*Model Bisnis WLAN di Indonesia*”, *Makalah Tugas Jaringan Nirkabel dan Bergerak (EI-7021)*, MTI-ITB, Desember 2003.
- [16] Chris N. Shepherd, “*Justify the Return on Security Investments to Company Stakeholders : Crafting a Quantifiable Business Case*”, ICCT Corp, Januari 2003. <http://www.icctcorp.com/>
- [17] John Hull, “*Option Markets*”, *Introduction to Futures and Options Markets*, Prentice Hall International Editions, 1991. Halm. 188-208, 229-250, 328-337.
- [18] Dan Latimore, “*Calculating Value During Uncertainty : Getting Real with Real Options*”, *IBM Institute for Business Value*, 2002. <http://www.ibm.com/services/strategy>

-
- [19] M. Benaroch dan Robert J. Kauffman, "A Case For Using Real Options Pricing Analysis To Evaluate Information Technology Project Investments", *Information Systems Research*, Vol.10, No.1, 1999, Hal.70-86
- [20] L.A. Gordon dan M.P. Loeb, "*Real Options and Security : The Wait-and-See-Approach*", *Computer Security Journal*, Vol.19, No.2, 2003.
- [21] Markus Dimpfel, Frank Habann dan Rene Algesheimer, "The Contribution of Real Options Theory to The Flexibility Management in Media Companies".
[Http://www.tukkk.fi/mediagroup/5WMEC%20PAPERS/Dimpfel%20&%20Habann%20&%20Algesheimer.pdf](http://www.tukkk.fi/mediagroup/5WMEC%20PAPERS/Dimpfel%20&%20Habann%20&%20Algesheimer.pdf)