ANALISA RESIKO KEAMANAN INFORMASI *(INFORMATION SECURITY)*. STUDI KASUS: POLIKLINIK XYZ

Dodi Wisaksono Sudiharto
Jurusan Teknik Informatika, Fakultas Informatika, Institut Teknologi Telkom
Jl. Telekomunikasi No. 1, Bandung 40257 Telp (022)-7565931
e-mail : dws@ittelkom.ac.id

Abstrak
Untuk menghadapi resiko yang mungkin terjadi terhadap keamanan informasi, maka resiko tersebut perlu untuk dimanajemen. Salah satu tindakan yang diperlukan dalam memanajemen resiko adalah menganalisa resiko yang mungkin terjadi. Beberapa perangkat yang dapat digunakan untuk menganalisa resiko adalah Single Lost Expectancy (SLE), Annualized Rate of Occurance (ARO), Exposure Factor (EF), Annual Loss Expectancy (ALE) dan Return on Investment (ROI).

Kata Kunci*: Single Lost Expectancy, Annual Loss Expectancy, Annualized Rate of Occurance, Exposure Factor dan Return on Investment.*

1. PENDAHULUAN

Salah satu resiko hal dihadapi organisasi adalah resiko yang mungkin terjadi terhadap keamanan informasi. Sehingga resiko tersebut perlu untuk dimanajemen. Salah satu tindakan yang diperlukan dalam memanajemen resiko adalah menganalisa resiko yang mungkin terjadi. Beberapa perangkat yang dapat digunakan untuk menganalisa resiko adalah *Single Lost Expectancy* (SLE), *Annualized Rate of Occurance* (ARO), *Exposure Factor* (EF), *Annual Loss Expectancy* (ALE) dan *Return on Investment* (ROI). Pada penelitian ini akan dilakukan analisa resiko terhadap keamanan informasi *(security information)* berbasis perangkat-perangkat tersebut pada Poliklinik XYZ.

Analisa resiko dibatasi hanya pada penanganan resiko yang terkait dengan kebakaran, pencurian, pemutusan layanan listrik, pemutusan layanan internet, pemutusan layanan telepon dan *virus/worm* pada Poliklinik XYZ.

2. TEORI DASAR

Manajemen resiko berarti melakukan tindakan untuk meminimalisir kemungkinan terjadinya resiko pada aset-aset perusahaan. Menghilangkan sama sekali resiko terhadap aset perusahaan adalah suatu hal yang tidak mungkin. Dari adanya resiko yang mungkin terjadi, ada beberapa parameter yang menjadi pertimbangan untuk dimanajemen. Di antara parameter tersebut adalah akibat *(impact)* dan probabilitas kejadian resiko itu sendiri. Sehingga kedua parameter tersebut dalam suatu analisa resiko, menjadi parameter yang diturunkan ke dalam perangkat analisa resiko. Selain itu, resiko juga dapat dihitung baik secara kualitatif dan kuantitatif.

Sebelum menganalisa resiko secara mendalam, biasanya dilakukan analisa resiko secara kualitatif terlebih dahulu [2]. Untuk menganalisa resiko secara kualitatif, terdapat *adjective* atau nilai asumsi yang digunakan [2]. Umumnya nilai yang digunakan menggunakan batasan *high* (tinggi), *medium* (menengah) dan *low* (rendah). Batasan terhadap nilai tersebut kemudian diturunkan sebagai nilai dari ALE *(Annual Loss Expectancy)* [2]. Agar suatu nilai kuantitatif dapat dikonversi ke dalam nilai kualitatif tersebut, digunakan batasan nilai yang umumnya dalam satuan finansial. Misalnya sebagai berikut [2]:

Tabel 1. Tabel *adjective* (nilai asumsi).

ALE *(Annualized Rate of Occurance)*	**Nilai Finansial**
Very Low (Sangat Rendah)	Lebih dari £1,000
Low (Rendah)	£1,000 - £ 10,000
Low/Medium (Rendah/Menengah)	£10,000 - £50,000
Medium (Menengah)	£ 50,000 - £100,000
Medium/High (Menengah/Tinggi)	£100,000 - £500,000
High (Tinggi)	500,000 - £1,000,000

Analisa resiko secara kuantitatif dilakukan berbasis parameter akibat *(impact)* dan probabilitas kejadian resiko. Nilai ini kemudian diturunkan sebagai nilai dari SLE *(Single Lost Expectancy)* [3]. Nilai SLE adalah nilai perkiraan terkait kerugian finansial yang muncul tatkala terjadi satu kali bencana *(disaster)* [3].

ARO *(Annualized Rate of Occurance)* adalah estimasi frekuensi resiko yang terjadi dalam satu tahun [1]. Sebagai contoh, estimasi terjadinya kebakaran pada organisasi adalah sekali dalam 30 tahun. Maka nilai ARO-nya adalah 1/30 atau 3,33%.

EF *(Exposure Factor)* adalah estimasi terhadap tingkat *(degree)* dari kehilangan aset *(asset loss)* akibat bencana [1]. Sebagai contoh, estimasi kehilangan aset akibat kebakaran pada organisasi adalah 70%. Maka nilai EF-nya adalah 0,7 atau 70%.

Nilai aset atau AV *(Asset Value)* umumnya direpresentasikan ke dalam satuan moneter atau finansial. Yang dimaksud dengan aset adalah apa pun baik materiil maupun imateriil yang menjadi pendukung berjalannya kegiatan organisasi [1].

Sehingga, nilai SLE bila diturunkan akan menjadi [6]:

$$SLE = AV \times EF$$

Sedangkan hubungan SLE dan ALE diturunkan menjadi [5]:

$$ALE = SLE \times ARO$$

ROI *(Return on Investment)* adalah rasio nilai perolehan suatu investasi relatif terhadap jumlah nilai yang diinvestasikan. Pada analisa resiko keamanan informasi (information security), ROI digunakan untuk mengambil keputusan apakah suatu tindakan penanganan resiko hasil analisa resiko pantas untuk dieksekusi. Kepantasan tersebut adalah bila ROI memiliki nilai lebih atau sama dengan 2:1 [3]. Bila diturunkan maka menjadi [4]:

$$ROI = (ALE_{current} - ALE_{projected}) / Annual\ Cost\ Investation$$

$ALE_{current}$ di mana adalah estimasi ALE saat belum dilakukan tindakan penanggulangan terhadap resiko, sedangkan $ALE_{projected}$ adalah estimasi ALE saat setelah dilakukan tindakan penanggulangan terhadap resiko.

3. ANALISA

Penulis melakukan analisis resiko dengan studi kasus Poliklinik XYZ. Poliklinik XYZ adalah sebuah poliklinik yang memberikan pelayanan berupa konsultasi dokter dan apotek. Dokter praktek di poliklinik ini terdiri dari 3 bagian, yaitu dokter umum, dokter gigi dan bidan. Poliklinik XYZ telah memiliki sistem informasi rekam medis lengkap dengan infrastruktur jaringan yang mendukung sistem tersebut.

Tabel *adjective* yang digunakan untuk estimasi ALE untuk Poliklinik XYZ adalah sbb:

Tabel 2. Tabel *adjective* estimasi ALE untuk Poliklinik XYZ

ALE *(Annualized Rate of Occurance)*	**Nilai Finansial**
Very Low (Sangat Rendah)	Rp 0 – Rp 10.000.000
Low (Rendah)	Rp 10.000.000 – Rp 100.000.000
Low/Medium (Rendah/Menengah)	Rp 100.000.000 – Rp500.000.000
Medium (Menengah)	Rp 500.000.000 – Rp 1.000.000.000
Medium/High (Menengah/Tinggi)	Rp 1.000.000.000 – Rp 5.000.000.000
High (Tinggi)	>Rp 5.000.000.000

Aset yang dimiliki oleh Poliklinik XYZ terdiri dari aset gedung dan aset selain gedung. Dari daftar aset hasil identifikasi, penulis melakukan analisa resiko. Dari analisa ini diharapkan akan didapatkan nilai ROI untuk mengetahui apakah tindakan penanganan resiko memiliki kepantasan untuk dieksekusi.

Berikut ini adalah daftar estimasi ALE, dikelompokkan berdasarkan perkiraan resiko yang akan terjadi, yaitu akibat terjadinya kebakaran, pencurian, pemutusan layanan listrik, pemutusan layanan internet, pemutusan layanan telepon dan *virus/worm*. Nilai ROI juga disertakan sesuai kategori resiko yang ditangani.

A. Kebakaran

Diperkirakan dalam 10 tahun terjadi 1 kali kebakaran. Kejadian ini akan berdampak pada kerusakan fisik dan terhentinya suatu layanan. Nilai ARO yang digunakan adalah 1/10 = 0,1

Tabel 3. *ALE current* untuk resiko kebakaran.

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Gedung		5.000.000.000	5.000.000.000	Fisik	70	3.500.000.000	0,1	350.000.000
2	Alat Kesehatan Umum	3	1.200.000	3.600.000	Fisik	100	3.600.000	0,1	360.000
3	Meja Periksa	2	2.000.000	4.000.000	Fisik	60	2.400.000	0,1	240.000
4	Dental Unit	1	35.000.000	35.000.000	Fisik	80	28.000.000	0,1	2.800.000
5	ADSL Router	1	500.000	500.000	Fisik	50	250.000	0,1	25.000
6	Server Database	1	7.000.000	7.000.000	Fisik	50	3.500.000	0,1	350.000
7	PC Client	10	2.000.000	20.000.000	Fisik	50	10.000.000	0,1	1.000.000
8	Printer 1	2	400.000	800.000	Fisik	50	400.000	0,1	40.000
9	Printer 2	5	1.200.000	6.000.000	Fisik	50	3.000.000	0,1	300.000
10	LAN	1	5.000.000	5.000.000	Fisik	100	5.000.000	0,1	500.000
11	UPS	10	500.000	5.000.000	Fisik	50	2.500.000	0,1	250.000
12	Telepon	3	150.000	450.000	Fisik	50	225.000	0,1	22.500
13	Software Medical Record		50.000.000	50.000.000		20	10.000.000	0,1	1.000.000
14	Data Poliklinik		20.000.000	20.000.000		50	10.000.000	0,1	1.000.000
15	Stok Obat		500.000.000	500.000.000	Fisik	80	400.000.000	0,1	40.000.000
16	Laba Layanan Poliklinik		60.000.000	60.000.000		25	15.000.000	0,1	1.500.000
								Total Kerugian Per Tahun	399.387.500

Tindakan yang diambil untuk mengurangi resiko kemungkinan terjadinya kebakaran (menjadi nilai *Annual Cost Investation*):

Tabel 4. Penanganan resiko kebakaran

No	**Tindakan Penanganan**	**Biaya (Rp)**
1	Pembelian alat pemadam kebakaran sejumlah 6 buah @ Rp 1.500.000	9.000.000
2	Pemasangan Alarm asap 12 @ Rp 150.000 + Pemasangan	2.000.000
3	Asuransi Kebakaran	7.500.000
4	Pembelian Harddisk Eksternal untuk Backup Data	1.000.000
Total		21.500.000

Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Estimasi $ALE_{projected}$ menjadi sebagai berikut:

Tabel 5. *ALE projected* untuk resiko kebakaran

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{projected}$ (Rp)
1	Gedung		5.000.000.000	5.000.000.000	Fisik	0.2	10.000.000	0,1	1.000.000
2	Alat Kesehatan Umum	3	1.200.000	3.600.000	Fisik	50	1.800.000	0,1	180.000
3	Meja Periksa	2	2.000.000	4.000.000	Fisik	0	0	0,1	0
4	Dental Unit	1	35.000.000	35.000.000	Fisik	20	7.000.000	0,1	700.000
5	ADSL Router	1	500.000	500.000	Fisik	0	0	0,1	0
6	Server Database	1	7.000.000	7.000.000	Fisik	25	1.750.000	0,1	175.000
7	PC Client	10	2.000.000	20.000.000	Fisik	25	5.000.000	0,1	500.000
8	Printer 1	2	400.000	800.000	Fisik	0	0	0,1	0
9	Printer 2	5	1.200.000	6.000.000	Fisik	0	0	0,1	0
10	LAN	1	5.000.000	5.000.000	Fisik	50	2.500.000	0,1	250.000
11	UPS	10	500.000	5.000.000	Fisik	10	500.000	0,1	50.000
12	Telepon	3	150.000	450.000	Fisik	0	0	0,1	0
13	Software Medical Record		50.000.000	50.000.000		1	500.000	0,1	50.000
14	Data Poliklinik		20.000.000	20.000.000		1	200.000	0,1	20.000
15	Stok Obat		500.000.000	500.000.000	Fisik	10	50.000.000	0,1	5.000.000
16	Laba Layanan Poliklinik		60.000.000	60.000.000		1	600.000	0,1	60.000
								Total Kerugian Per Tahun	7.985.000

Sehingga dari data di atas didapatkan nilai ROI: (399.387.500 – 7.985.000) / 21.500.000 = 18,20 ~ 18 : 1

B. Pencurian

Diperkirakan dalam 1 tahun terjadi 1 kali pencurian. Kejadian ini akan berdampak pada aset yang bersifat fisik. Nilai ARO yang digunakan adalah 1/1 = 1

Tabel 6. *ALE current* untuk resiko pencurian

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Dental Unit	1	35.000.000	35.000.000	Fisik	100	35.000.000	1	35.000.000
2	ADSL Router	1	500.000	500.000	Fisik	100	500.000	1	500.000
3	Server Database	1	7.000.000	7.000.000	Fisik	50	3.500.000	1	3.500.000
4	PC Client	10	2.000.000	20.000.000	Fisik	50	10.000.000	1	10.000.000
5	Printer 1	2	400.000	800.000	Fisik	50	400.000	1	400.000
6	Printer 2	5	1.200.000	6.000.000	Fisik	50	3.000.000	1	3.000.000
7	UPS	10	500.000	5.000.000	Fisik	50	2.500.000	1	2.500.000
8	Telepon	3	150.000	450.000	Fisik	50	225.000	1	225.000
9	Stok Obat		500.000.000	500.000.000	Fisik	5	25.000.000	1	25.000.000
Total Kerugian Per Tahun									80.125.000

Tindakan yang diambil untuk mengurangi resiko kemungkinan terjadinya pencurian (menjadi nilai *Annual Cost Investation*):

Tabel 7. Penanganan resiko pencurian

No	**Tindakan Penanganan**	**Biaya (Rp)**
1	Penambahan 1 orang anggota satpam untuk *shift* malam	12.000.000
2	Teralis besi untuk tiap jendela	10.000.000
3	Pemasangan kamera 4 cctv @ Rp 500.000 + pemasangan	2.500.000
Total		24.500.000

Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang karena frekuensi pencurian menurun menjadi 1 kali pencurian dalam 10 tahun. Sehingga nilai ARO = 1/10 = 0,1. Estimasi $ALE_{projected}$ menjadi sebagai berikut:

Tabel 8. *ALE projected* untuk resiko pencurian

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{projected}$ (Rp)
1	Dental Unit	1	35.000.000	35.000.000	Fisik	100	35.000.000	0,1	3.500.000
2	ADSL Router	1	500.000	500.000	Fisik	100	500.000	0,1	50.000
3	Server Database	1	7.000.000	7.000.000	Fisik	50	3.500.000	0,1	350.000
4	PC Client	10	2.000.000	20.000.000	Fisik	50	10.000.000	0,1	1.000.000
5	Printer 1	2	400.000	800.000	Fisik	50	400.000	0,1	40.000
6	Printer 2	5	1.200.000	6.000.000	Fisik	50	3.000.000	0,1	300.000
7	UPS	10	500.000	5.000.000	Fisik	50	2.500.000	0,1	250.000
8	Telepon	3	150.000	450.000	Fisik	50	225.000	0,1	22.500
9	Stok Obat		500.000.000	500.000.000	Fisik	5	25.000.000	0,1	2.500.000
Total Kerugian Per Tahun									8.012.500

Sehingga dari data di atas didapatkan nilai ROI: (80.125.000 – 8.012.500) / 24.500.000 = 2,94 ~ 3 : 1

C. Pemutusan Aliran Listrik

Diperkirakan terjadi 6 kali pemadaman listrik dalam setahun. Maka ARO = 6/1 = 6.

Tabel 9. *ALE current* untuk resiko pemutusan aliran listrik

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Laba Layanan Poliklinik	1	60.000.000	60.000.000		50	30.000.000	6	180.000.000
Total Kerugian Per Tahun									180.000.000

Tindakan yang diambil untuk mengurangi resiko dengan melakukan pembelian genset (menjadi nilai *Annual Cost Investation*):

Tabel 10. Penanganan resiko pemutusan aliran listrik

No	Tindakan Penanganan	Biaya (Rp)
1	Generator	12.000.000
2	Bensin	1.000.000
Total		13.000.000

Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang karena tidak pernah mengalami pemadaman. Sehingga nilai ARO = 0. Estimasi $ALE_{projected}$ menjadi sebagai berikut:

Tabel 11. *ALE projected* untuk resiko pemutusan aliran listrik

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{projected}$ (Rp)
1	Laba Layanan Poliklinik	1	60.000.000	60.000.000		0,5	300.000	0	0
Total Kerugian Per Tahun									0

Sehingga dari data di atas didapatkan nilai ROI: (180.000.000 – 0) / 13.000.000 = 13,8 ~ 14 : 1

D. Pemutusan Layanan Internet

Diperkirakan terjadi 6 kali dalam 1 tahun terjadi gangguan layanan internet. Maka ARO = 6/1 = 6.

Tabel 12. *ALE current* untuk resiko pemutusan layanan internet

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Layanan Internet		11.000.000	11.000.000		0,1	110.000	6	660.000
Total Kerugian Per Tahun									660.000

Untuk pemutusan layanan internet belum dapat ditemukan tindakan yang dapat meminimalisasi resiko tersebut. Namun nilai ALE termasuk relatif sangat kecil *(very low).*

E. Pemutusan Layanan Telepon

Diperkirakan terjadi 1 kali pemutusan layanan telepon dalam 2 tahun. Maka ARO = 1/2 = 0,5.

Tabel 13. *ALE current* untuk resiko pemutusan layanan telepon

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Layanan Telepon		7.000.000	7.000.000		0,1	700.000	0,5	350.000
Total Kerugian Per Tahun									350.000

Untuk pemutusan layanan telepon belum dapat ditemukan tindakan yang dapat meminimalisasi resiko tersebut. Namun nilai ALE termasuk relatif sangat kecil *(very low).*

F. Virus / Worm

Diperkirakan terjadi 6 kali gangguan *software* akibat *virus/worm* dalam setahun. Maka ARO = 6/1 = 6.

Tabel 14. *ALE current* untuk resiko *virus/worm*

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Software Medical Record		50.000.000	50.000.000		20	10.000.000	6	60.000.000
2	Data Poliklinik		20.000.000	20.000.000		50	10.000.000	6	60.000.000
Total Kerugian Per Tahun									120.000.000

Resiko di atas dapat dikurangi dengan melakukan migrasi sistem operasi komputer ke sistem operasi Linux. Dampak migrasi ini adalah diperlukannya *training* untuk semua *user*. Berikut ini adalah tindakan penanganan yang diambil (menjadi nilai *Annual Cost Investation*):

Tabel 15. Penanganan resiko *virus/worm*

No	Tindakan Penanganan	Biaya (Rp)
1	Melakukan migrasi ke sistem operasi Linux	10.000.000
2	Training dasar Linux untuk 10 orang @ Rp 600.000	6.000.000
Total		16.000.000

Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Estimasi $ALE_{projected}$ menjadi sebagai berikut:

Tabel 16. *ALE current* untuk resiko *virus/worm*

No	Item	Jml	Nilai Satuan (Rp)	Nilai Total (Rp)	Klasifikasi	EF (%)	SLE (Rp)	ARO (Rp)	$ALE_{current}$ (Rp)
1	Software Medical Record		50.000.000	50.000.000		1	500.000	1	500.000
2	Data Poliklinik		20.000.000	20.000.000		50	10.000.000	1	10.000.000
Total Kerugian Per Tahun									10.500.000

Sehingga dari data di atas didapatkan nilai ROI: (120.000.000 – 10.500.000) / 16.000.000 = 6,8 ~ 7 : 1

4. KESIMPULAN

1). Nilai ROI atas estimasi terhadap tindakan penanggulangan yang lebih besar dari 2 : 1 didapatkan pada analisa resiko untuk:
   a). Kebakaran, sebesar 18 : 1.
   b). Pencurian, sebesar 3 : 1.
   c). Pemutusan aliran listrik, sebesar 14 : 1.
   d). Penanganan *virus/worm*, sebesar 7 : 1

2). Nilai ROI atas estimasi tindakan penanggulangan kebakaran, pencurian, pemutusan aliran listrik dan penanganan *virus/worm*, menjadikan tindakan penanggulangan tersebut memiliki kepantasan untuk dieksekusi, karena nilainya lebih besar dari 2 : 1.

3). Untuk resiko pemutusan layanan internet dan pemutusan layanan telepon tidak memiliki estimasi tindakan penanggulangan atas resiko. Namun hal tersebut berpengaruh sangat kecil terhadap keberlangsungan operasional organisasi, karena ALE atas resiko yang mungkin muncul sangat rendah *(very low).*

5. DAFTAR PUSTAKA

[1]. Davis, C., Mike Schillerand, M, Wheeler K. (2007): IT Auditing: Using Controls to Protect Information Assets, McGraw-Hill, Bab 15

[2]. Palmer, I.C. & G.A. Potter. (1989): *"Computer Security Risk Management"*. Van Nostrand Reinhold., halaman 215.

[3]. Palmer, I.C. & G.A. Potter. (1989): *"Computer Security Risk Management"*. Van Nostrand Reinhold., halaman 218.

[4]. Palmer, I.C. & G.A. Potter. (1989): *"Computer Security Risk Management"*. Van Nostrand Reinhold., halaman 226.

[5]. ___, *Annualized Loss Expectancy.* <http://www.riskythinking.com/glossary/annualized_loss_expectancy.php>. Diakses Juni 2011.

[6]. ___, *Single Loss Expectancy.* <http://www.riskythinking.com/glossary/single_loss_expectancy.php>. Diakses Juni 2011.