STRATEGI MITIGASI RESIKO KEAMANAN INFORMASI BERDASARKAN ANALISA *RETURN ON INVESTMENT* PADA BADAN PUSAT STATISTIK DAERAH KOTA SEMARANG

Asih Rohmani[1], Muhammad Gunawan Wibisono[2]
[1,2] Program Studi Sistem Informasi Fakutas Ilmu Komputer Universitas Dian Nuswantoro
Jl.Nakula I No. 1 – 11 Semarang 50131
Telp. : (024) 3517261, Fax : (024) 3520165
Email: aseharsoyo@dsn.dinus.ac.id[1], 112201405224@mhs.dinus.ac.id[2]

Abstrak

Informasi merupakan aset penting perusahaan yang harus dilindungi dari berbagai bentuk ancaman dan serangan. Secara garis besar, ancaman terhadap sistem informasi berupa ancaman aktif dan ancaman pasif.Strategi untuk mengamankan aset informasi bisa dilakukan oleh perusahaan atau organisasi dengan cara menyusun mitigasi resiko berdasarkan identifikasi aset perusahaan dan identifikasi serangan yang mungkin terjadi. Salah satu metode yang digunakan adalah metode kuantitatif dengan analisa berdasarkan nilai ROI. Analisa ini berdasarkan kejadian yang pernah terjadi dalam periode tertentu. Hal pertama yang dilakukan adalah mengidentifikasi aset beserta nilai nominalnya dan mengidentifikasi kejadian disertai perkiraan kerugian akibat kejadian tersebut, dalam hal ini nilai kerugian menjadi nilai Single Lost Expectancy (SLE). Selanjutnya menentukan estimasi prosentase dari kehilangan aset yang diekspresikan dalam nilai Exposure Factor (EF). Dari dua variabel tersebut ditambah nilai estimasi frekuensi kejadian satu tahun atau Annualized Rate of Occurance (ARO) akan menghasilkan nilai estimasi kerugian per tahun atau Annual Loss Expectancy (ALE). Analisa berlanjut pada kemungkinan tindakan yang diambil untuk mengurangi resiko ancaman, hingga akhirnya ditemukan nilai Return On Investment (ROI) yang menjadi panduan apakah kemungkinan-kemungkinan tindakan tersebut pantas untuk diterapkan atau tidak.

***Kata kunci**: vulnerability, analisa resiko kuantitatif, return on investment*

Abstract

Information is an important company asset that must be protected from various forms of threats and attacks. Broadly speaking, threats to information systems in the form of threats of active and passive threat. Strategies for securing information assets can be done by a company or organization by arranging the mitigation of risk by identifying the company's assets and the identification of possible attack. One method used is quantitative analysis method based on the value of ROI. This analysis is based on events that have occurred in a given period. The first thing to do is to identify assets and their nominal value and identify events with estimates of losses due to the incident, in this case the value of the loss into the value Single Lost Expectancy (SLE). Next determine the estimated percentage of loss of assets expressed in value Exposure Factor (EF). Of the two variables plus the estimated value of the frequency of one year or Annualized Rate of Occurance (ARO) would result in estimated losses per year or Annual Loss Expectancy (ALE). Analysis continues on the possible measures taken to reduce the risk of threats, until finally found the value of Return On Investment (ROI) is a guide to whether the possibilities of such actions deserve to be applied or not.

***Keywords**: vulnerability, quantitative risk analysis, return on investment*

1. PENDAHULUAN

Keamanan informasi merupakan hal penting yang masih sangat jarang diperhatikan oleh perusahaan atau organisasi sebagai pemilik informasi tersebut. Hasil survey *ESET Asia Cyber Savviness Report 2015* mengungkap fakta bahwa negara Indonesia menempati urutan terendah pengetahuan masyarakatnya terhadap resiko kejahatan *cyber*. Selain itu, masyarakat Indonesia juga tercatat 'santai' saja terhadap ancaman *cybercrime* dan dinilai yang paling tidak khawatir terhadap kejahatan di dunia *online*.[1]

Informasi merupakan aset penting perusahaan yang harus dilindungi dari berbagai bentuk ancaman dan serangan. Secara garis besar, ancaman terhadap sistem informasi bisa dibagi menjadi dua kategori yaitu ancaman aktif, seperti kejahatan atau kecurangan yang dilakukan dengan sengaja oleh seseorang, dan ancaman pasif yang berupa kegagalan sistem, kesalahan manusia yang tidak disengaja dan faktor bencana alam.[2]

Schechter mendefinisikan istilah umum keamanan sebagai "proses identifikasi peristiwa yang memiliki potensi untuk menyebabkan bahaya (atau skenario ancaman) dan menerapkan perlindungan untuk mengurangi atau menghilangkan potensi ini ". Keamanan dapat dilihat sebagai proses mempertahankan aset terhadap kerusakan atau bahaya. [3]

Dalam rangka mengembangkan strategi yang tepat untuk mencegah terjadinya suatu peristiwa, sebuah perusahaan atau organisasi bisa melakukannya dengan cara menyusun mitigasi resiko berdasarkan identifikasi aset perusahaan yang disertai dengan identifikasi serangan yang mungkin terjadi. Resiko adalah suatu kesempatan yang berdampak negatif. Perusahaan dapat memperkecil resiko, namun tidak mungkin dapat sepenuhnya menghindari resiko, bahkan dengan struktur pengendalian maksimal sekalipun. Analisa terhadap resiko pada dasarnya menggunakan pendekatan *risk management*, yang digunakan untuk membantu mengidentifikasi ancaman dan memilih kriteria ukuran keamanan yang menghasilkan *cost effectif*. [4]

Analisa resiko secara kuantitatif dilakukan berdasarkan parameter akibat *(impact)* dan probabilitas kejadian resiko, sehingga kedua parameter tersebut dalam suatu analisa resiko kuantitatif menjadi parameter yang diturunkan ke dalam perangkat analisa resiko.[5]

Badan Pusat Statistik (BPS) Daerah Kota Semarang merupakan BPS daerah yang melaksanakan tugas pokok sehubungan dengan penyimpanan data-data statistik yang dibebankan oleh BPS pusat. BPS Daerah Kota Semarang memiliki visi dan misi yaitu menyediakan informasi statistik yang lengkap dan akurat. Dalam kegiatan pengumpulan dan pengolahan data, BPS menggunakan bantuan *software* aplikasi *Microsoft Excel* dalam proses rekap data dan kemudian menginputkan data tersebut ke dalam *database* BPS pusat. Pengolahan data awal dengan menggunakan bantuan perangkat lunak aplikasi perkantoran (bukan perangkat lunak pengolah data) ini rentan terhadap kesalahan manusia dan resiko kehilangan. Proses transformasi data ke dalam *database* BPS pusat juga memberikan peluang terjadinya ancaman. Berkaitan dengan hal tersebut, maka keamanan aset informasi menjadi hal yang sangat penting.

Terkait dengan permasalahan tersebut, tujuan penelitian ini adalah untuk melakukan analisa resiko keamanan aset

informasi sehingga memperoleh hasil yang berguna untuk pencegahan terjadinya resiko keamanan informasi

2. METODE PENELITIAN

Dalam penelitian ini metode yang akan digunakan penulis adalah metode analisa resiko kuantitatif.

2.1 Perhitungan Analisa Resiko Kuantitatif

Variabel kunci dan persamaan yang dipergunakan untuk melaksanakan suatu analisis resiko kuantitatif adalah sebagai berikut [6] :

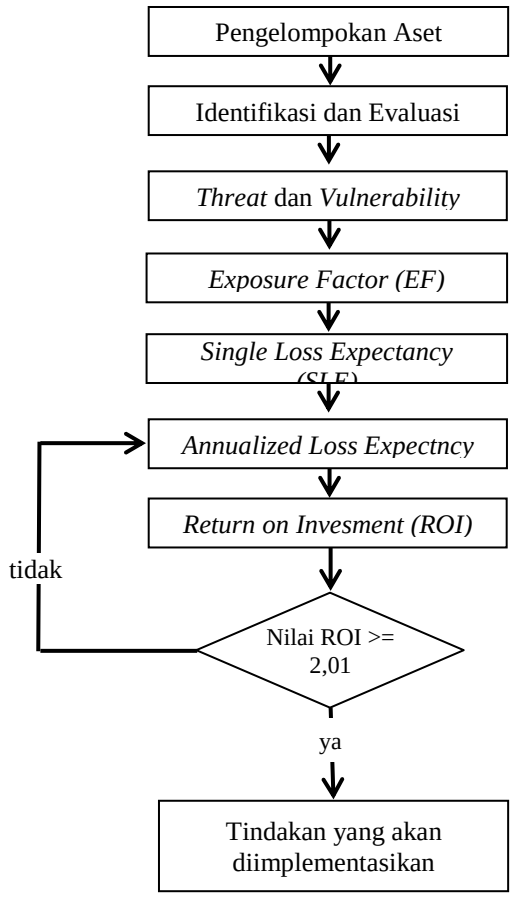
1. *Exposure Factor* (EF) : Persentase suatu kehilangan aset(*asset loss)* yang disebabkan oleh identifikasi ancaman. Rentang nilainya antara 0% sampai 100%.
2. *Single Loss Expectancy* (SLE) adalah nilai kerugian terhadap aset bila sebuah resiko yang teridentifikasi terjadi.

   SLE = *Asset Value* x *Exposure Factor* (EF)
3. *Annualized Rate of Occurrence* (ARO) adalah perkiraan atau estimasi frekuensi sebuah resiko yang dapat terjadi dalam setahun. Apabia sebuah resiko terjadi sekali dalam 10 tahun, maka nilai ARO adalah 0,1.
4. *Annualized Loss Expectancy* (ALE) adalah nilai estimasi kerugian pertahun terhadap aset, jika sebuah resiko yang teridentifikasi terjadi. Nilai ALE ada dua yaitu ALE *current* (ALE sebelum menerapkan *safeguards*) dan ALE *projected* (ALE setelah menerapkan *safeguards*).

   ALE = SLE x ARO
5. *Return On Investment* (ROI) adalah rasio nilai perolehan suatu investasi relatif terhadap sejumlah nilai yang diinvestasikan. Pada analisa resiko keamanan informasi, ROI digunakan untuk mengambil keputusan apakah suatu tindakan penanganan resiko hasil analisa resiko pantas untuk dilaksanakan atau tidak.

   ROI = *(ALE current – ALE projected) / Annual Cost Investation*

Data diperoleh dari hasil wawancara dengan beberapa staf dan pimpinan di BPS Daerah Kota Semarang. Berikut adalah langkah-langkah dalam melakukan analisa resiko terhadap aset pada BPS:



Gambar 1. Metode Kuantitatif Analisa Resiko Aset Informasi. Sumber [7]

2.2 Pengelompokan Aset

Dalam pengelompokan aset, langkah pertama yang dilakukan adalah menggambaran lingkup perusahaan. BPS memiliki jenis aset perkantoran.

Kemudian aset perkantoran tersebut diidentifikasi seperti aset jenis TI dan sumber daya informasi yang menjadi dasar sistemnya. Dari hasil analisis aset BPS dikelompokkan menjadi 4 jenis aset, yaitu:

a. Aset informasi, terdiri dari data karyawan, data survey, data keuangan.
b. Aset fisik terdiri dari server, PC, laptop printer,perangkat jaringan, TV, kamera, motor, mobil, proyektor, telepon dan gedung.
c. Aset software, terdiri dari sistem operasi, aplikasi perkantoran.
d. Aset orang, terdiri dari karyawan dan tenaga *outsourcing*.

2.3 Identifikasi dan Valuasi Aset

Berdasarkan analisa aset pada BPS dan formula perhitungan analisis secara kuantitatif, maka didapatkan hasil sebagai berikut:

Tabel 1: Valuasi Aset [Sumber: BPS Daerah Kota Semarang]

No	Aset	Jumlah	Nilai Satuan (ribuan Rp)	Total (ribuan Rp)
1	Gedung	1	600.000	600.000
2	Server IBM	1	49.000	49.000
3	Layanan Internet	1	500	500
4	PC Notebook: Thinkpad T420	8	15.700	125.600
5	Printer Canon Pixma MX897	3	2.750	8.250
6	PC Desktop: Dell Vostro 460 MT	15	7.661	114.915
7	Layar Proyektor SONY VPL-EX100	2	6.786	13.572
8	Kamera Canon 1200 D	2	4.500	9.000
9	Access Point: TP-LINK TL-WA901ND	2	400	800
10	Karyawan Outsourching	5	1.100	5.500
11	Data Survey	1.000	1	1.000
12	Operating System	23	1.700	39.100
13	Meja dan Kursi	35	912	31.920
14	Kabel LAN	15	40	600

2.4 Klasifikasi Ancaman Keamanan Informasi pada BPS Daerah Kota Semarang

Tujuan dari langkah ini adalah untuk mengidentifikasi potensi dari sumber ancaman dan melakukan penyusunan suatu daftar yang memaparkan ancaman potensi sumber ancaman. Sumber ancaman digambarkan sebagai suatu keadaan atau peristiwa yang memiliki potensi dapat menyebabkan kerusakan. Sumber ancaman berasal dari alam, manusia dan lingkungan.

Tabel 2: Ancaman kemanan informasi pada BPS Daerah Kota Semarang

Ancaman	**Klasifikasi**	**ARO**	**Source**	**C**	**I**	**A**
Kebakaran	Bencana	0,2	Wawancara			x
Pencurian	Sengaja	3		x		x
Rusak Secara Fisik	Tidak Sengaja	10				x
Virus / *Malcode / Malware*	Sengaja	20			x	x
Layanan Internet Down	Tidak Sengaja	4				x

2.5 *Exposure Factor (EF)*

Estimasi terhadap tingkat (*degree*) dari kehilangan aset (*asset loss*) akibat bencana. Presentasi penilaian suatu kehilangan aset yang disebabkan oleh identifikasi ancaman, rentang nilai estimasinya antara 0% sampai 100%.

Tabel 3: Estimasi Nilai EF

Value	**Deskripsi**

0 %	Aset tahan terhadap ancaman
0 % s/d < 20 %	Kerusakan kecil
20 % s/d < 40 %	Tingkat kerusakan menengah, akan terjadi delay dalam pekerjaan
40 % s/d < 60 %	Tingkat kerusakan besar, akan terjadi delay dalam pekerjaan
60 % s/d < 80 %	Tingkat kerusakan besar, pekerjaan sudah mengalami interupsi
80 % s/d 100 %	Kerusakan fatal, pekerjaan terhenti dan sistem membutuhkan total *replacement*

3. HASIL DAN PEMBAHASAN

Berdasarkan daftar aset hasil identifikasi dan valuasi aset yang tertera pada tabel 1, maka dilakukan analisa resiko kuantittif. Dari hasil analisa diharapkan akan didapatkan nilai ROI untuk mengetahui apakah tindakan atau *safeguards* penanganan resiko memiliki kepantasan untuk diterapkan atau tidak. Menurut Palmer dalam [7], suatu tindakan pantas dilakukan apabila nilai ROI >= 2,01 atau 2:1.
Berikut hasil perhitungan EF, ARO, ALE *Current*, ALE *Projected* dan ROI.

3.1 Ancaman Kebakaran

Dalam lima tahun terakhir terjadi kebakaran sebanyak satu kali. Kebakaran tersebut tidak terlalu besar sehingga proses bisnis pada BPS tidak terhenti.

Tabel 4: ALE *Current* Kebakaran

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Current* (ribuan Rp)
Gedung	Kecelakaan	10%	60.000	0,2	12.000
Meja dan Kursi	Kecelakaan	5%	1.596	0,2	319,2
				Total	12.319,2

Dari data diatas didapatkan nilai ROI:

ROI = (12.319,2 - 3.791,52) / 6.833,5

ROI = 1,25

3.2 Ancaman Pencurian

Dalam satu tahun terakhir terjadi pencurian sebanyak tiga kali.

Tabel 5: ALE *Current* Pencurian

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Current* (ribuan Rp)
Printer Epson	Kesengajaan	30 %	5.675,76	3	17.027,28
PC Desktop : Dell Vostro 430	Kesengajaan	10 %	12.560	3	37.680
Kamera Canon 1200 D	Kesengajaan	3 %	270	3	810
Motor Honda CB 100	Kesengajaan	20 %	8.400	3	25.200
Layar Proyektor SONY VPL-EX100	Kesengajaan	40 %	3.437,68	3	10.313,04
				Total	91.030,32

Tindakan yang akan diambil BPS untuk mengurangi resiko kemungkinan terjadi pencurian adalah sebagai berikut (menjadi nilai *Annual Cost Investment*):

Tabel 6: Rencana Tindakan Pencegahan Terhadap Ancaman Pencurian

No	Tindakan	Biaya (ribuan Rp)
1	Penabahan satu orang penjaga atau satpam untuk shif malam	8.400
2	Memasang teralis besi pada setiap jendela	10.000
3	Pemasangan kamera CCTV 1 paket (recording , terdiri dari 4 unit) + biaya pasang	5.000
	Total	23.400

Setelah dilakukan tindakan penangan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang dan EF juga berkurang. Estimasi ALE *Projected* menjadi sebagai berikut:

Tabel 7: ALE *Projected*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Projected* (ribuan Rp)
Printer Epson	Kesengajaan	10 %	1.891,92	3	5.675,76
PC Desktop : Dell Vostro 430	Kesengajaan	5 %	6.280	3	18.840
Kamera Canon 1200 D	Kesengajaan	2 %	180	3	540
Motor Honda CB 100	Kesengajaan	10 %	4.200	3	12.600
Layar Proyektor SONY VPL-EX100	Kesengajaan	20 %	1.718,84	3	5.156,52
				Total	42.812,28

Dari data diatas didapatkan nilai ROI:

ROI = (91.030,32- 42.812,28) / 23.400

ROI = 2,06

3.3 Kerusakan Aset Secara Fisik

Dalam satu tahun terakhir terjadi kerusakan aset fisik sebanyak sepuluh kali.

Tabel 8: ALE *Current* Kerusakan Aset Secara Fisik

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Current* (ribuan Rp)
Printer Epson	Tidak sengaja	10 %	1.891,92	10	18.919,2
PC Desktop : Dell Vostro 430	Tidak sengaja	40 %	57.000	10	570.000
Layar Proyektor SONY VPL-EX100	Tidak sengaja	20 %	1.718,84	10	17.188,4
Access Point: TP-LINK TL-WA901 ND	Tidak sengaja	50 %	400	10	4.000
				Total	610.107,6

Tindakan yang akan diambil BPS untuk mengurangi resiko kemungkinan terjadi kerusakan aset fisik adalah sebagai berikut (menjadi nilai *Annual Cost Investment*):

Tabel 9: Rencana Tindakan Pencegahan Terhadap Ancaman Pencurian

No	Tindakan	Biaya (ribuan Rp)
1	Pelatihan penggunaan perangkat keras dengan benar	20.000
2	Pembelian tempat penyimpanan untuk pengamanan aset	30.000
3	Mendatangkan tenaga outsourcing untuk perbaikan asset	20.000
	Total	70.000

Setelah dilakukan tindakan penangan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang dan EF juga berkurang. Estimasi ALE *Projected* menjadi sebagai berikut:

Tabel 10: ALE *Projected*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Projected* (ribuan Rp)
Printer Epson	Tidak sengaja	5 %	945,96	10	9.459,6
PC Desktop: Dell Vostro 430	Tidak sengaja	20 %	28.500	10	285.000
Layar Proyektor SONY VPL-EX100	Tidak sengaja	10 %	859,42	10	8.594,2
Access Point: TP-LINK TL-WA901ND	Tidak sengaja	20 %	160	10	1.600
				Total	304.653,8

Dari data diatas didapatkan nilai ROI:

ROI = (610.107,6- 304.653,88) / 70.000

ROI = 8,58

3.4 Ancaman Virus / *Malcode* / *Malware*

Dalam satu tahun terakhir terjadi kerusakan akibat virus / *malcode / malware* sebanyak dua puluh kali.

Tabel 11: ALE *Current* Ancaman Virus / *Malcode/ Malware*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Current* (ribuan Rp)
PC Desktop : Dell Vostro 430	Tidak sengaja	7 %	9.975	20	199.500
PC Notebook: Dell Thinkpad T420	Tidak sengaja	3 %	3.768	20	75.360
				Total	274.860

Tindakan yang diambil BPS untuk mengurangi resiko kemungkinan Ancaman Virus / *Malcode / Malware* adalah sebagai berikut (menjadi nilai *Annual Cost Investment*):

Tabel 12: Rencana Tindakan Pencegahan Terhadap Ancaman Virus / *Malcode / Malware*

No	Tindakan	Biaya (ribuan Rp)
1	Pembeliasn antivirus premium	1.500
2	*Maintenance* secara berkala	20.000

	menggunakan tenaga *outsourching*	
	Total	21.500

Setelah dilakukan tindakan penangan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang dan EF juga berkurang. Estimasi ALE *Projected* menjadi sebagai berikut:

Tabel 13: ALE *Projected*Ancaman Virus / *Malcode / Malware*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Projected* (ribuan Rp)
PC Desktop : Dell Vostro 430	Tidak sengaja	4 %	5.700	20	114.000
PC Notebook: Dell Thinkpad T420	Tidak sengaja	2 %	2.512	20	50.240
				Total	164.240

Dari data diatas didapatkan nilai ROI:

ROI = (274.860- 164.240) / 21.500

ROI = 5,15

3.5 Layanan Internet *Down*

Dalam satu tahun terakhir terjadi layanan internet *down* sebanyak empat kali.

Tabel 14: ALE *Current* Layanan Internet *Down*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Current* (ribuan Rp)
Layanan internet	Tidak sengaja	40 %	960	4	3.840
				Total	3.840

Tindakan yang akan diambil BPS untuk mengurangi resiko kemungkinan Ancaman Layanan Internet *Down* adalah sebagai berikut (menjadi nilai *Annual Cost Investment*):

Tabel 15: Rencana Tindakan Pencegahan Terhadap Layanan Internet Down

No	Tindakan	Biaya (ribuan Rp)
1	Pindah ISP	6.000
	Total	6.000

Setelah dilakukan tindakan penangan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang dan EF juga berkurang. Estimasi ALE *Projected* menjadi sebagai berikut:

Tabel 16: ALE *Projected*Layanan Internet *Down*

Item	Klasifikasi	EF	SLE (ribuan Rp)	ARO	ALE *Projected* (ribuan Rp)
Layanan internet	Tidak sengaja	20 %	480	4	1.920
				Total	1.920

Dari data diatas didapatkan nilai ROI:

ROI = (3.840 - 1.920) / 6.000

ROI = 0,32

Tabel 17: Nilai ROI

No	Ancaman	ROI
1	Kebakaran	0,56
2	Pencurian	2,42
3	Rusak secara fisik	8,58
4	Virus/Malicious	5,15

	Code/Malware	
5	Layanan Internet Down	0,32

Ancaman yang memiliki nilai ROI lebih besar dari 2,01 adalah pencurian, rusak secara fisik dan virus / *malcode / malware*, sehingga perencanaan untuk mitigasi resiko yang sudah dianalisa pantas untuk diterapkan. Sedangkan mitigasi resiko terhadap ancaman kebakaran dan layanan internet down kurang pantas untuk diterapkan karena biaya yang dikeluarkan untuk tindakan *safeguards* terlalu tinggi dibandingkan dengan *ALE current* dan *ALE projected*.

Dari analisa tersebut di atas, maka dibuat tabel strategi mitigasi resiko dan *vulnerability asset*. *Risk mitigation* adalah suatu metodologi yang digunakan oleh manajemen guna mengurangi resiko dari misi yang dibuat [2]. Sedangkan *vulnerability* adalah kelemahan yang ada pada aset dalam suatu organisasi. *Vulnerability* tidak menyebabkan rusaknya suatu aset, melainkan menciptakan suatu kondisi yang dapat mengakibatkan ancaman terjadi [2]

Berikut tabel strategi mitigasi resiko dan *vulnerability asset* pada BPS Daerah Kota Semarang:

Tabel 18: Strategi mitigasi resiko dan *vulnerability asset* pada BPS Daerah Kota Semarang

No	Risk		Strategi	Tindakan
	Threat	*Vulnerability*		
1	Kebakaran	Penanganan kebakaran BPS masih sangat lambat karena belum memiliki alat untuk menanggulangi kebakaran	Menghindari resiko dengan melakukan penanganan terhadap penyebab resiko dan membuat standar kebijakan pengamanan aset	Pembelian alat pemadam kebakaran dan pemasangan alarm asap
2	Pencurian	Security BPS belum aksimal karena masih mengandalkan penjaga kantor saja		Penambahan seorang satpam atau penjaga dan pemasangan CCTV serta memasang teralis besi di tiap jendela kantor
3	Rusak secara fisik	Karyawan BPS masih beum memahami standar penggunaan komputer dan perangkat yang lain dengan benar		Pelatihan karyawan, membeli tempat penyimpanan aset dan mendatangkan tukang servis
4	Code/ Malware	Banyak komputer yang terkena virus meskipun sudah ada program antivirus		Pembelian antivirus premium dan *maintenance* secara berkala
5	Down	Layanan intnet yang digunakan pernah mengalami gangguan		Melakukan penggantian ISP

4. KESIMPULANDAN SARAN

4.1 Kesimpulan

Masalah keamanan sistem informasi tidak hanya bergantung pada tools atau perangkat pengamanan saja, melainkan bisa disiasati dengan penyusunan langkah-langkah pencegahan terjadinya ancaman ataupun serangan terhadap sistem itu sendiri, yang sering disebut dengan mitigasi resiko. Mitigasi resiko bisa disusun oleh perusahaan yang bersangkutan dengan cara mengidentifikasi aset yang dimiliki,

sekaligus mengidentifikasi ancaman yang mungkin terjadi terhadap aset tersebut.

Salah satu metode yang digunakan untuk menyusun mitigasi resiko keamanan informasi adalah dengan melakukan analisa resiko kuantitatif berdasarkan *cost effective*, yaitu dengan menghitung kerugian biaya aset dan biaya yang dibutuhkan untuk melakukan pencegahan. Apabila dari hasil analisa menunjukkan bahwa biaya yang dikeluarkan untuk pencegahan lebih besar daripada biaya kerugian atas kehilangan atau kerusakan aset, maka tindakan pencegahan tersebut tidak pantas untuk diterapkan.
Dari hasil analisa di kantor BPS Daerah Kota Semarang didapatkan bahwa tindakan pencegahan yang pantas untuk diterapkan adalah tindakan pencegahan terhadap ancaman pencurian, ancaman kerusakan perangkat secara fisik dan ancaman virus / *malcode / malware*, dimana masing-masing memiliki nilai ROI 2,42 ; 8,58 dan 5,15.

4.2 Saran

Informasi menghasilkan banyak rekomendasi tentang bagaimana cara mengamankan informasi sebagai salah satu aset terpenting perusahaan atau organisasi, namun meskipun begitu masih banyak celah yang bisa mengancam keamanan informasi. Begitu juga dengan hasil penelitian yang telah dilakukan dengan analisa resiko kuantitatif ini, maka akan lebih maksimal hasilnya apabila dalam penerapannya dikolaborasikan dengan metode yang lain. Adapun beberapa saran perbaikan untuk penelitian selanjutnya, adalah :

1. Identifikasi aset perlu dilakukan terhadap seluruh aset, termasuk aset-aset yang dianggap kecil, karena, bisa jadi aset yang tidak teridentifikasi justru berpotensi menimbulkan ancaman yang sulit untuk ditanggulangi.
2. Perlu diadakan kajian untuk mengetahui tipe perusahaan seperti apakah yang cocok menggunakan metode analisa kuantitatifdalam melakukan analisa resiko keamanan sistem informasi.
3. Variabel yang digunakan untuk analisis resiko keamanan informasi bisa lebih bervariasi lagi sehingga bisa menghasilkan hasil analisa yang lebih akurat.

DAFTAR PUSTAKA

[1] ESET Asia Cyber-Savviness Report 2015, 2015,*Cyber Security: User Knowledge, Behaviour and Attitudes In Asia.*

[2] Paryati, 2008, Keamanan Sistem Informasi, Proceding Seminar Nasional Informatika 2008 (semnasIF 2008), ISSN: 1979-2328, Yogyakarta.

[3] Neubauer,T., Hartl, C., 2009, On the singularity of valuating IT security investments, In: *Eigth IEEE/ACIS International Conference on Computer and Information Science*, IEEE Computer Society.

[4] Supradono, B. , 2009, Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*), Media Elektrika, Vol. 2, No. 1.

[5]Sudiharto,D.W., 2011 Analisa Resiko Keamanan Informasi (*Information Security*). Studi Kasus: Poliklinik XYZ, Seminar Nasional Informatika 2011 (semnasIF 2011) ISSN: 1979-2328, Yogyakarta.

[6] Tan,D., 2013, *Quantitative Risk Analysis Step-By-Step*, SANS Institute

[7] Soebijono, T., 2012, Analisa Resiko Keamanan InformasiSebagai Strategi Mitigasi ResikoPada Toko Online "X", SNASTI.