ANALISIS STRATEGI PENGELOLAAN KEAMANAN INFORMASI MENGGUNAKAN PEMODELAN SISTEM DINAMIK

Eko Martantoh
Teknik Informatika, STMIK Cikarang
Email: eko6379@yahoo.co.id

Abstrak

Penanganan pengelolan keamanan informasi merupakan hal yang mutlak dilakukan pada organisasi yang memiliki sistem informasi dalam menunjang operasional organisasi. Sistem informasi yang terdiri dari aset baik perangkat lunak maupun perangkat keras yang mengelola data dan informasi yang tersebar melalui jaringan dan internet, menjadikannya rentan terhadap ancaman. Oleh karena itu dibutuhkan investasi dan biaya untuk mengamankannya. Biaya yang dikeluarkan untuk keperluan ini tidaklah kecil, tetapi pengeluaran investasi dan biaya keamanan informasi yang dilakukan perlu penanganan yang serius agar lebih efektif dan tepat sasaran. Model Sistem Dinamik digunakan untuk mengevaluasi alternatif strategi untuk menunjukkan efektifitas investasi dan biaya pengelolaan keamanan informasi melalui simulasi perubahan kebijakan. Sistem dinamik adalah metode untuk menggambarkan model dan manganalisis sistem yang bersifat dinamis dan komplek, yang terdiri dari variabel yang saling mempengaruhi dalam bentuk hubungan sebab-akibat dan umpan balik antar variabel baik yang bersifat menguatkan atau memberi keseimbangan. Simulasi menggunakan model sistem dinamik pada penelitian ini menggambarkan bahwa pengelolaan penilaian resiko yang diikuti oleh usaha pengurangan kerentanan memiliki dampak yang sangat besar terhadap pengelolaan keamanan informasi. Dengan membuat perbedaan nilai variabel probabiltas pengurangan kerentanan, maka hal ini memberikan pilihan alternatif dalam investasi pengelolaan resiko keamanan informasi untuk mencapai efektifitas keseluruhan biaya yang dikeluarkan pada pengelolaan keamanan informasi.

Kata kunci: Information Security Management, System Dynamic, Simulation, Model, Pengelolaan Keamanan Informasi, Sistem Dinamik, Simulasi

I. PENDAHULUAN

Mengelola keamanan informasi adalah tugas yang sangat penting dan menantang. Organisasi memperbolehkan karyawan maupun orang lain untuk mengakses sistem informasi dari mana-mana, dengan kecanggihan ancaman keamanan yang semakin meningkat, kebutuhan untuk memberikan keamanan dianggap lebih penting. Pengelolaan keamanan informasi yang efektif memerlukan sumber daya keamanan yang mencakup berbagai bidang, termasuk pencegahan serangan, pencegahan ancaman, dan pengurangan kerentanan. Menggunakan model sistem dinamik akan memberikan strategi pengelolaan keamanan alternatif melalui sudut pandang biaya investasi.

Sistem dinamik digunakan untuk mengetahui implikasi keuangan terhadap keputusan organisasi dalam menentukan investasi aset keamanan informasi. Kemampuan untuk mengkorelasikan konstruksi dalam jangka waktu tertentu dan melacak perkembangan lintas waktu merupakan faktor penting dalam memilih metodologi simulasi sistem dinamik. Model ini dimaksudkan untuk mencakup kebijakan keamanan, kerentanan, dan serangan, mengkaitkannya dengan biaya keamanan dan kerusakan keseluruhan yang berkelanjutan. Model ini memberikan manajer dengan kemampuan untuk mengetahui pengaruh sumber daya menempatkannya ke dalam pilihan alternatif keamanan dan dampak dari keputusan di bawah berbagai kondisi. Meskipun model tidak dapat mencakup semua serangan keamanan dan skenario, model tersebut memberi manajer dengan wawasan pengorbanan risiko yang relatif. Penelitian ini mengadopsi metodologi ilmu desain menggunakan model sistem dinamik sebagai pembahasan yang menarik. Pemanfaatan pembahasan tersebut ditunjukkan melalui keberhasilan pelaksanaan model di bawah berbagai kondisi. Penelitian ini juga membahas pengelolaan dan implikasi penelitian model keamanan (D. L. Nazareth, J. Choi, 2014: 125).

Pendekatan metodologi sistem dinamik menunjukkan bagaimana struktur, kebijakan, keputusan dan penundaan waktu dengan sistem adalah saling terkait dan mempengaruhi dalam pertumbuhan dan stabilitas. Hal ini dianggap bahwa fungsi sistem ditentukan oleh struktur, dan pola perilaku sistem tergantung pada struktur dinamis dan mekanisme umpan balik internal dari sistem. Langkah pertama menerapkan pengelolaan keamanan informasi adalah membangun kebijakan keamanan informasi yang lengkap (Pei-Chen Sung, Chien-Yuan Su, 2013: 84).

Membangun diagram lingkar sebab-akibat dengan serangkaian faktor yang diidentifikasi, dan kemudian membangun model SD untuk mengungkapkan model penilaian resiko, berupa simulasi yang menghasilkan lima tipe resiko yaitu resiko sistem perangkat keras (*hardware risk system*), resiko sistem perangkat lunak (*sotware risk system*), resiko data (*data risk*), resiko lingkungan (*environment risk*), dan resiko manusia (*human risk*) (Liu Wei, et.al, 2015: 82).

Membangun model sistem dinamik untuk menganalisis perilaku menyimpang dan mengembangkan model deteksi ancaman dari dalam. Mengevaluasi strategi ancaman dari segi manusia, proses, dan teknologi. Model ini dibuat dengan tujuan untuk efisiensi dan mengefektifkan. (1) Pemantauan perilaku pengguna dalam operasional sistem informasi dan secara otomatis membangun profil perilaku pengguna. (2) Mengembangkan teknologi yang kompatibel untuk membedakan indikasi pemicu kemungkinan perilaku menyimpang. (3) Untuk mendeteksi kemungkinan perilaku menyimpang segera dan mengurangi waktu deteksi perilaku internal yang menyimpang. (4) Untuk meningkatkan efisiensi kerja pemantauan dan administrasi sistem dengan mengurangi sejumlah besar penyimpanan yang tidak berguna (Sang-Chin Yang, Yi-Lu Wang, 2011: 12).

Analisis hubungan antara undang-undang EFT (*Electronic Financial Transaction*) dan standar penilaian resiko serta mengusulkan peta area yang membantu lembaga keuangan untuk menentukan prioritas area kontrol keamanan menggunakan sistem dinamik dengan mengintegrasikan Standar keamamanan ISO 270001, KISA ISMS dan FISS. Menghasilkan model analisis sederhana menggunakan sistem dinamik untuk penilaian kebijakan, dengan menggunakan metode penilaian resiko untuk perusahaan finansial dengan mencoba mengintegrasikan standar keamanan informasi yang berbeda (Ae Chan Kim, et.al, 2012: 198).

Metodologi *option-based framework*, menyajikan aplikasi untuk sistem SHS (*Spridnings-och Hamnings System*: sistem penyebaran dan pencarian kembali informasi) secara rinci dan membandingkannya dengan praktek saat ini untuk menangani tiga informasi spesifik terkait masalah keamanan:

1. Eksternalitas keamanan informasi
2. Dinamisasi manajemen persyaratan keamanan
3. Evaluasi/re-evaluasi kebutuhan yang sedang berlangsung untuk keamanan IT/produk.

Kerangka berdasarkan pilihan dibuat dan disesuaikan dengan masalah keamanan IT tertentu sehingga mereka dapat dirumuskan dan dianalisa sesuai dengan pilihan teori. Pendekatan yang dihasilkan mampu menemukan nilai selama ketidakpastian untuk menyelidiki solusi optimal dari serangkaian alternatif dan memberikan bimbingan strategis untuk masalah manajemen keamanan informasi dalam lingkungan yang dinamis (Haider Abbas, et.al, 2010: 20).

Dalam jurnal penelitian ini akan menggunakan model sistem dinamik untuk pengelolaan keamanan informasi, dimana akan dilakukan modifikasi model pada penelitian sebelumnya dengan mencari variabel pengungkit (*leverage*) dan menambahkan variabel lain apabila diperlukan untuk keperluan analisis lebih lanjut. Pemodelan pengelolaan keamanan informasi dapat memperlihatkan bahwa simulasi menggunakan sistem dinamik memberi gambaran dalam bentuk konstruksi atau struktur, berupa skenario yang dikorelasikan dengan beberapa variabel penting sesuai dengan permasalahan yang dibahas dalam penelitian ini yaitu tentang pegelolaan keamanan informasi. Validasi dilakukan dengan membuat persamaan-persamaan yang disesuaikan perubahannya menurut waktu, yang kemudian akan tercipta sebuah hasil dasar sesuai dengan sekenario. Penelitian yang dilakukan oleh Haider Abbas, et.al menggunakan pendekatan *options-based framework* yang mampu menemukan nilai selama ketidakpastian untuk menyelidiki solusi optimal dari serangkaian alternatif dan memberikan bimbingan strategis untuk masalah manajemen keamanan informasi dalam lingkungan yang dinamis, dalam pendekatan ini pilihan sudah dibuat tetapi tingkat pengaruh dari setiap variabel tidak dijelaskan secara detail. Pemodelan simulasi sistem dinamik untuk pengelolaan keamanan informasi juga dikembangkan untuk dapat menganalisis strategi pengelolaan keamanan informasi dengan membuat alternatif-alternatif kebijakan yang sekiranya dapat dijadikan bahan untuk pengambilan keputusan yang lebih efisien. Dibandingkan dengan *options-based framework* sistem dinamik memberikan pilihan alternatif-alternatif kebijakan yang lebih banyak dan memiliki nilai pada setiap variabelnya yang dapat dinaikkan atau diturunkan nilainya sehingga berpengaruh terhadap variabel yang lain di dalam sistem.

II. LANDASAN TEORI

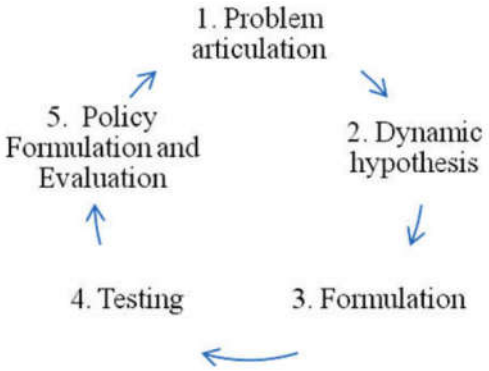
2.1. Pemodelan Sistem Dinamik

Sistem Dinamik (SD) adalah metode untuk menggambarkan model dan menganalisis sistem atau isu-isu dinamis yang komplek dalam hal proses, informasi, strategi dan batas-batas organisasi (Erik Pruyt, 2013: 1). Sistem dinamik mempelajari tentang perilaku sistem yang dinamis dan komplek dalam sebuah proses umpan balik yang terdiri dari *loop* penguatan (*reinforcing*) dan penyeimbang (*balancing*) (Miroljub Kljajić, et.al., 2012: 315). Sistem dinamik dikembangkan pada tahun 1950 oleh Jay W. Forrester of Massachusetts Institute of Technology (MIT). Kerangka kerja ini terfokus pada pemikiran sistem, tetapi mengambil langkah-langkah tambahan untuk membangun dan pengujian model simulasi. Suatu karakteristik utama dari metode ini adalah adanya sistem yang kompleks, perubahan perilaku sistem, dan adanya umpan balik *loop* tertutup untuk menggambarkan informasi baru mengenai kondisi sistem yang akan menghasilkan keputusan berikutnya. (Erma Suryani, et.al, 2010: 733).

Menggunakan model sistem dinamik, manajer dapat membuat "apa-jika" skenario dengan mengubah variabel untuk melihat bagaimana kinerja sistem akan diubah dan dapat menggunakan informasi tersebut untuk memanipulasi sistem untuk mencapai hasil yang diinginkan. (Deborah Marshall, et.al, 2010:4).

2.2. Prinsip Kerja Model Sistem Dinamik

Sterman di dalam (Erma Suryani, et.al, 2010: 734) telah mengembangkan langkah-langkah untuk membuat model sistem dinamik seperti yang digambarkan dalam Gambar 2.1.



Gambar 2.1. Langkah-langkah Membuat Model Sistem Dinamik

Langkah 1: Artikulasi masalah: pada langkah ini, kita perlu mencari masalah yang sebenarnya, mengidentifikasi variabel kunci dan konsep, menentukan horizon waktu dan ciri masalah dinamis untuk memahami dan merancang kebijakan untuk menyelesaikannya.

Langkah 2: Hipotesis dinamis: pemodel harus mengembangkan teori tentang bagaimana masalah muncul. Pada langkah ini, kita perlu mengembangkan diagram lingkaran sebab akibat yang menjelaskan hubungan kausal antara variabel dan mengubah diagram causal loop ke dalam diagram alir, yang terdiri dari beberapa variabel.

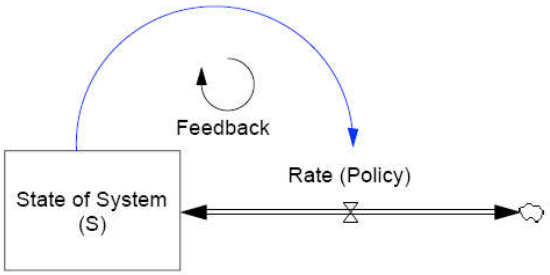
Langkah 3: Formulasi: untuk menentukan model system dinamik, setelah mengubah diagram causal loop ke dalam diagram alir, kemudian menerjemahkan deskripsi sistem ke tingkat penambahan persamaan. Perlu untuk memperkirakan beberapa parameter, hubungan perilaku, dan kondisi awal. Menulis persamaan akan mengungkapkan kesenjangan dan inkonsistensi yang harus diperbaiki dalam deskripsi sebelumnya.

Langkah 4: Pengujian: tujuan pengujian adalah untuk membandingkan perilaku simulasi model terhadap perilaku aktual dari sistem.

Langkah 5: Perumusan dan evaluasi kebijakan: setelah pemodel mengembangkan kepercayaan dalam struktur dan perilaku model, model yang valid dapat dimanfaatkan untuk merancang dan mengevaluasi kebijakan untuk perbaikan. Interaksi kebijakan yang berbeda juga harus dipertimbangkan, karena sistem real sangat nonlinear dan dampak kombinasi kebijakan biasanya tidak hanya satu dampak saja.

2.3. **Notasi Pemodelan Sistem Dinamik**

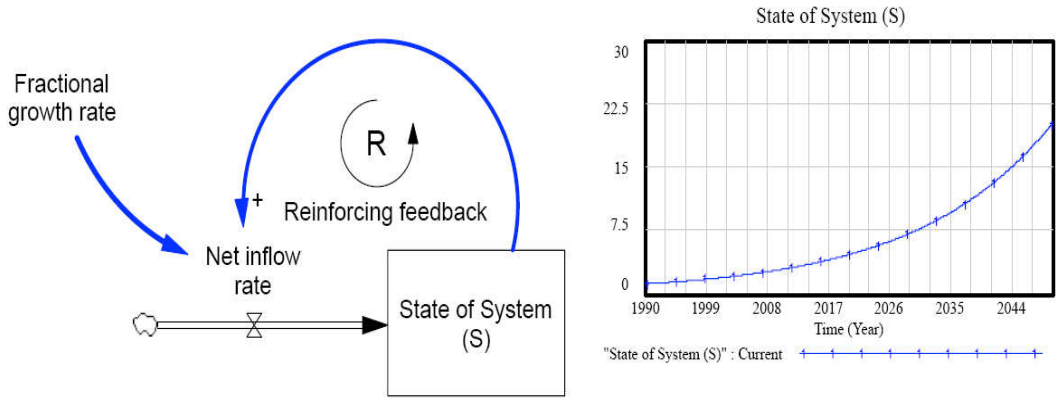
Konsep dasar dalam sistem dinamik adalah bahwa keadaan sistem adalah *self-modifying* terhadap *feedback* dan dapat digambarkan secara visual yang terlihat pada gambar 2.2 (Dr Michael Yearworth, 2014:7).



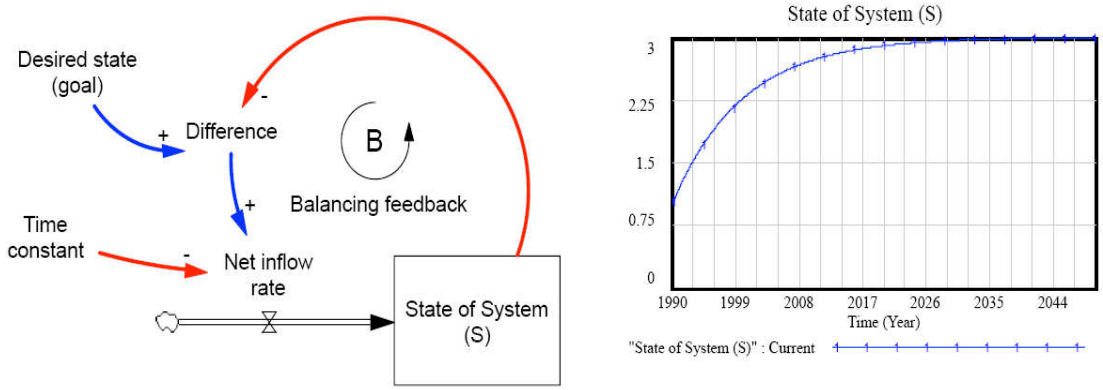
Gambar 2.2 Konsep Dasar Sistem Dinamik – *self-modifying state according to feedback.*

Persegi panjang menyatakan stok, kuantitas dari sistem yang merupakan subjek yang terakumulasi, dan atau pengurangan akumulasi menurut tingkat arus masuk maupun keluar stok yang ditunjukkan oleh simbol katup. Simbol awan menunjukkan batas sistem. Hal ini menunjukkan bahwa sumber atau tenggelamnya dari arus adalah berada di luar sistem.

Reinforcing Diagram ditunjukkan pada gambar 2.3. dan memperlihatkan pertumbuhan eksponensial di dalam *state variable*. Gambar 2.4. memperlihatkan perilaku mencapai tujuan dari *balancing feedback.*



Gambar 2.3. *Reinfforcing Feedback* Mengarahkan ke Pertumbuhan Eksponensial.



Gambar 2.4. Balancing Feedback Mengarahkan ke Pencapaian Tujuan atau Perilaku Control.

III. HASIL PENELITIAN

3.1. Pemodelan Sistem Dinamik untuk Pengelolaan Keamanan Informasi

Penggerak dari sebagian besar investasi dan kontrol keamanan informasi adalah ancaman dan serangan. Setiap organisasi terutama organisasi yang bergerak dalam bidang bisnis yang berorientasi profit selalu menyiapkan image yang baik untuk organisasinya. Target yang akan diserang memiliki nilai tertentu bagi penyerang, apakah target yang diserang memberikan keuntungan bagi penyerang secara langsung atau secara tidak langsung penyerang mendapatkan keuntungan dari pihak ketiga untuk menjatuhkan image organisasi karena persaingan bisnis. Image organisasi dikombinasikan dengan nilai target yang dirasakan akan membentuk daya tarik target. Serangan diawali oleh daya tarik target, dimana organisasi akan menyiapkan target agar tidak rentan terhadap serangan karena pertimbangan serangan sukses yang terjadi. Probabilitas serangan terbentuk oleh daya tarik target dalam hubungannya dengan motivasi penyerang, kerentanan yang dirasakan pada aset informasi organisasi, serta mekanisme pencegahan yang ada. Semua faktor penentu memiliki pengaruh positif terhadap probabilitas penyerang, kecuali mekanisme pencegahan yang memiliki efek penyeimbang terhadap probabilitas serangan.

Serangan dapat berasal dari dalam dan luar organisasi. Jumlah penyerang dan ketersediaan alat untuk menyerang akan mempengaruhi jumlah serangan yang terjadi. Diharapkan jumlah serangan yang masuk mampu terdeteksi oleh kemampuan deteksi sehingga dapat dicegah dan diakumulasi, sisanya adalah serangan yang sukses. Serangan yang sukses akan terjadi dalam berbagai bentuk dan memiliki efek yang berbeda. Beberapa akan menyebabkan kerusakan dan sebagian lainnya hanya mendekati kerusakan. Serangan yang sukses akan ditangkap dan dibuatkan laporannya. Laporan serangan tidak hanya terbentuk dari serangan sukses saja tetapi juga dipengaruhi oleh kerusakan dan mendekati kerusakan untuk mengetahui tingkat laporan serangan. Akumulasi laporan serangan akan menentukan kerentanan yang dirasakan dari aset informasi organisai, sehingga menyelesaikan lingkaran serangan. Ini adalah lingkaran (*loop*) yang semakin menguat, menunjukkan bahwa serangan sukses akan menyebabkan peningkatan laporan serangan.

Lingkaran kerentanan muncul akibat dari lingkaran serangan dimana perlu dilakukan usaha untuk mengurangi kerentanan diawali dengan melakukan usaha penilaian resiko. Usaha penilaian resiko dilakukan dengan melihat kerusakan aset informasi dan aset informasi yang hampir

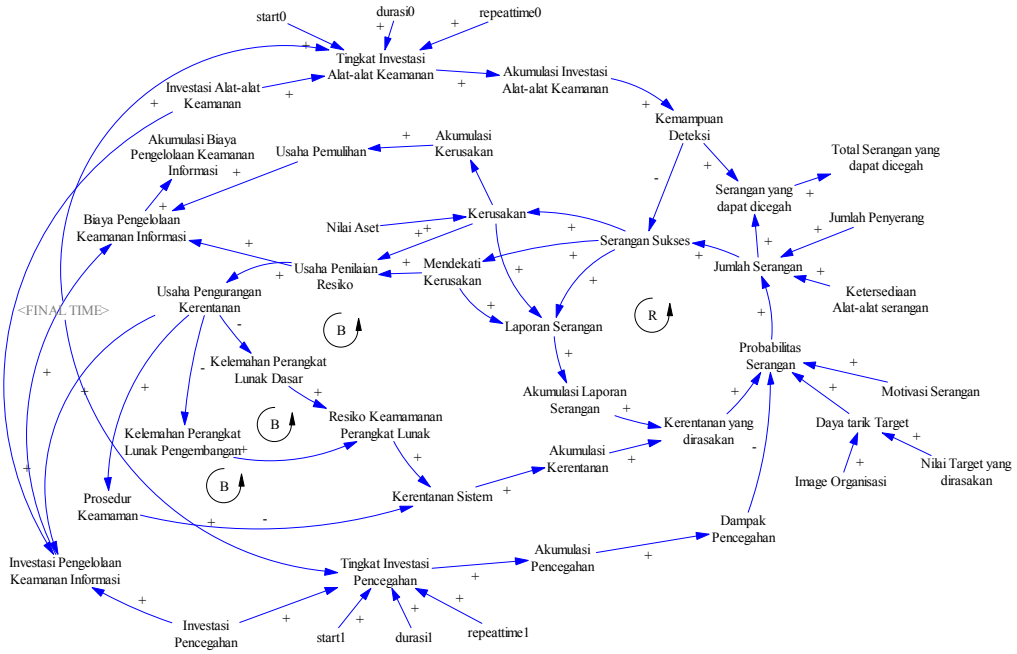
rusak. Usaha ini merupakan usaha penilaian baru bukan merupakan penilaian ulang, karena menilai kerentanan baru. Dengan ditemukannya kerentanan baru ini maka perlu dilakukan usaha untuk mengurangi kerentanan tersebut. Kerentanan di dalam lingkaran ini adalah adalah kerentanan pada perangkat lunak baik perangkat lunak dasar maupun perangkat lunak hasil pengembangan.

Seperti ditunjukkan di dalam diagram, kerentanan ini berbanding terbalik dengan usaha pengurangan kerentanan, yang menunjukkan bahwa diharapkan usaha ini dapat mengurangi kerentanan pada perangkat lunak dasar maupun pada perangkat lunak pengembangan. Kerentanan perangkat lunak dasar dikombinasikan dengan kerentanan perangkat lunak pengembangan akan menentukan resiko keamanan perangkat lunak secara keseluruhan. Usaha pengurangan kerentanan akan menimbulkan peningkatan pada prosedur keamanan. Kerentanan sistem ditentukan melalui efek gabungan dari prosedur keamanan dan resiko keamanan perangkat lunak. Prosedur keamanan memiliki hubungan terbalik dengan kerentanan sistem, implementasi yang efektif dari prosedur keamanan akan memperkecil kerentanan sistem. Sebaliknya resiko keamanan perangkat lunak digambarkan sebagai hubungan linier positif sehingga akan meningkatkan kerentanan sistem. Pada kasus yang berbeda prosedur keamanan yang tidak efektif dikombinasikan dengan resiko keamanan perangkat lunak yang signifikan menimbulkan kerentanan yang semakin buruk. Kerentanan sistem akan membentuk kerentanan yang dirasakan. Kerentanan yang dirasakan didasarkan pada laporan akumulasi kerentanan. Kerentanan yang dirasakan akan meningkatkan probabiltas serangan sehingga menyelesaikan lingkaran ini. Ini adalah lingkaran (*loop*) *balancing* dan akan cenderung mencari keseimbangan dan akan mempengaruhi lingkaran penguatan pada serangan.

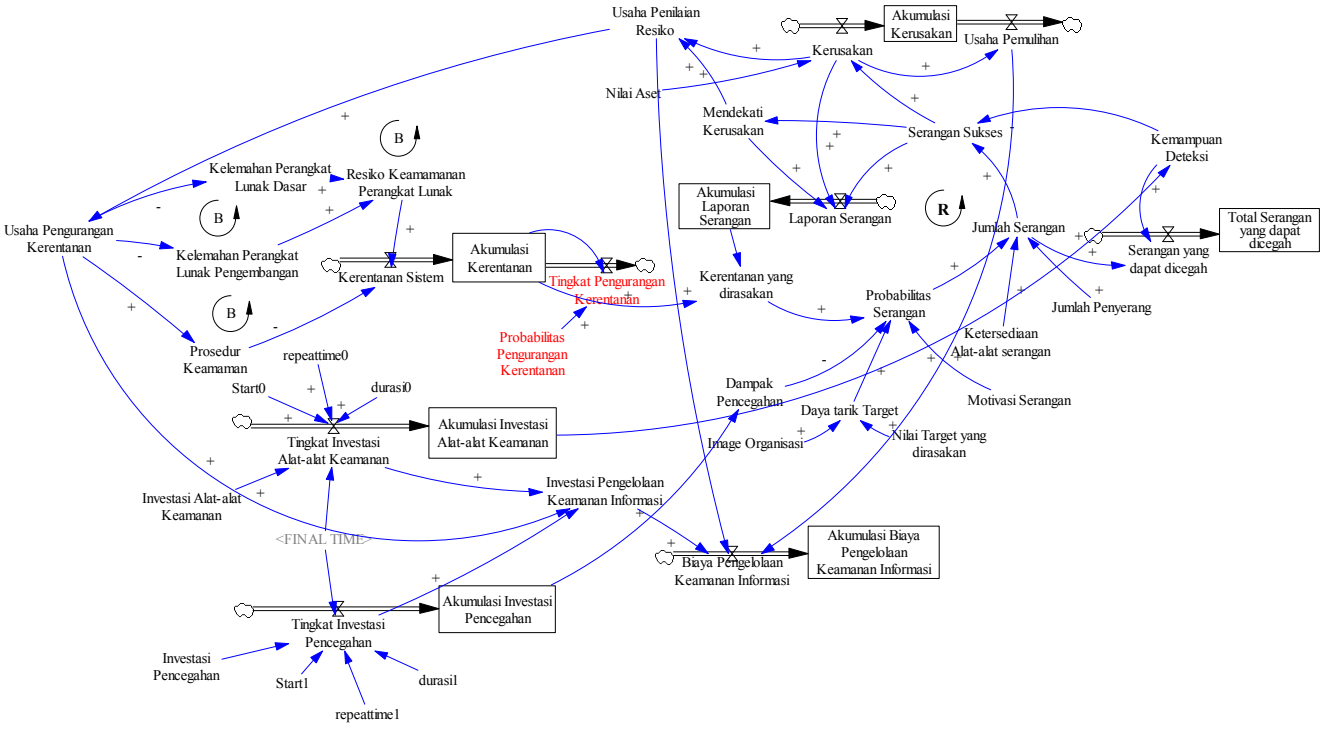
Organisasi berinvestasi dalam tindakan pencegahan, pengadaan alat-alat keamanan untuk mendeteksi dan mencegah serangan. Investasi ini dilakukan oleh organisasi dan dimulai (*start*) pada waktu yang ditentukan. Investasi juga memiliki batasan yang ditandai dengan adanya durasi dalam melakukan investasi, interval (*repeat time*) investasi, dan ini akan berakhir sesuai dengan batas akhir dari simulasi (*final time*). Investasi ini memiliki efek yang terus berlanjut sehingga menimbulkan akumulasi investasi. Akumulasi investasi alat-alat serangan menentukan kemampuan untuk mendeteksi dan menggagalkan serangan. Demikian pula, akumulasi pencegahan membentuk dampak pencegahan, yang memiliki hubungan dengan lingkaran serangan.

Investasi pada alat-alat keamanan dan pencegahan dikombinasikan dengan usaha pengurangan kerentanan, ini merupakan investasi pengelolaan keamanan informasi bagi organisasi yang berkontribusi pada biaya pengelolaan keamanan informasi. Usaha Pemulihan dilakukan dengan melihat akumulasi kerusakan yang terjadi yang muncul dari lingkaran serangan. Usaha pemulihan dan usaha penilaian resiko lebih lanjut berkontribusi terhadap Biaya Pengelolaan Keamanan Informasi perusahaan secara keseluruhan. Kemudian biaya pengelolaan keamanan informasi diakumulasi untuk mengetahui pertumbuhan biaya pengelolaan keamanan informasi dari waktu ke waktu.

Gambar 3.1 memperlihatkan causal loop diagram pengelolaan keamanan informasi secara keseluruhan. Lingkaran serangan yang merupakan lingkaran penguatan, dipengaruhi oleh beberapa variabel input seperti kemampuan deteksi yang memiliki fungsi untuk mendeteksi serangan yang masuk dan mampu untuk mencegahnya, kemudian dipengaruhi pula oleh tindakan pencegahan sehingga mempengaruhi probabilitas serangan yang menyebabkan berkurangnya jumlah serangan, dan tampak pula lingkaran kerentanan yang merupakan penyeimbang dari lingkaran serangan. Keluaran dari lingkaran serangan adalah terjadi beberapa kerusakan dan diikuti oleh usaha-usaha, seperti usaha pemulihan dan usaha penilaian resiko yang merupakan biaya pengelolaan keamanan informasi. Hasil ini nantinya akan digunakan untuk tahap selanjutnya yaitu membangun diagram alir atau model simulasi *stock & flow diagram* dengan menggunakan program komputer Vensim.



Gambar 3.1. *Causal Loop Diagram* Pengelolaan Keamanan Informasi



Gambar 3.2. Model Sistem Dinamik Pengelolaan Keamanan Informasi

4. PEMBAHASAN DAN HASIL

4.1 Deskripsi Pemodelan Sistem Dinamik Dengan Vensim

Model sistem dinamik dibangun berdasarkan *causal loop* yang sebelumnya telah dibuat. Dengan menggunakan program aplikasi vensim kemudian dibuatlah Model Sistem

Dinamik Pengelolaan Keamanan Informasi, seperti tampak pada gambar 3.2.

Model tersebut dibuat sedemikian rupa dengan membentuk *stock/level*, *rate*, *auxiliary* dan konstanta. *Stock* digambarkan dengan persegi panjang, yang merupakan akumulasi dari aliran data yang mengarah kepadanya. *Stock* juga terdapat aliran yang mengarah keluar yang menandakan bahwa informasi di dalam *stock* juga ada suatu pengurangan. *Rate* adalah satu-satunya variabel yang mempengaruhi *stock* dan digambarkan dengan simbol katup. *Auxiliary* adalah konstanta-konstanta lain sebagai variabel input. Untuk mempermudah dalam memahami konstruksi, model terdiri dari beberapa bagian yaitu serangan, kerentanan, investasi dan biaya pengelolaan keamanan informasi. Ketiga bagian ini bukanlah bagian yang terpisah melainkan bagian saling berhubungan. Konstruksi dari model ini dibuat agar dapat menggambarkan perilaku sistem sesuai dengan dunia nyata.

Pada model serangan digambarkan terdiri dari tiga *stock* yaitu, total serangan yang dapat dicegah, akumulasi kerusakan, dan akumulasi laporan serangan. Total serangan yang dapat dicegah muncul akibat adanya kemampuan deteksi, sebagai nilai probabilitas *rate* serangan yang dapat dicegah dari jumlah serangan. Kemampuan deteksi muncul akibat adanya tindakan investasi alat-alat keamanan. Jadi dengan adanya investasi alat-alat keamanan tidak semua jumlah serangan merupakan serangan sukses, tetapi beberapa akan menjadi serangan yang dapat dicegah. Akumulasi kerusakan dipengaruhi oleh kerusakan dan digambarkan oleh *rate* kerusakan yang timbul akibat serangan sukses yang terjadi. Nilai dari kerusakan tergantung dari nilai aset yang diserang. Akumulasi kerusakan ini nantinya menimbulkan biaya yang digambarkan oleh *rate* usaha pemulihan. Selain usaha pemulihan dibutuhkan pula usaha penilaian resiko untuk dapat menilai bagian-bagian sistem mana yang rentan terhadap serangan sehingga nantinya dapat dilakukan usaha pengurangan kerentanan sesuai dengan hasil penilaian resiko yang dilakukan. Akumulasi laporan serangan didapatkan dari *rate* laporan serangan yang berasal dari serangan sukses baik yang menyebabkan kerusakan atau serangan yang mendekati kerusakan. Pada kelompok kerentanan hanya terdapat satu *stock* yaitu Akumulasi kerentanan. Kerentanan ini terakumulasi dari rate kerentanan sistem yang merupakan kombinasi dari resiko keamanan perangkat lunak dan prosedur keamanan. Pada kelompok Investasi dan biaya pengelolaan keamanan informasi terdapat tiga *stock* yaitu akumulasi investasi alat-alat keamanan, akumulasi investasi pencegahan, dan akumulasi biaya pengelolaan keamanan informasi. Akumulasi investasi alat-alat keamanan terakumlasi oleh *rate* tingkat investasi alat-alat keamanan, yang merupakan investasi yang dilakukan untuk meningkatkan kemampuan deteksi keamanan. Pada *rate* inilah yang pada pembahasan sebelumnya telah dilakukan sedikit modifikasi agar perubahan konstanta dapat dilakukan lebih interaktif. Modifikasi ini juga dilakukan pada *rate* tingkat investasi pencegahan sebagai variabel yang mempengaruhi *stock* akumulasi pencegahan dimana stock ini menimbulkan dampak pencegahan sebagai efek penyeimbang probabilitas serangan. *Stock* berikutnya adalah biaya pengelolaan keamanan informasi yang merupakan indikator penting untuk memperlihatkan seberapa besar biaya yang dikeluarkan untuk pengelolaan keamanan informasi secara keseluruhan. *Stock* ini dipengaruhi oleh *rate* biaya pengelolaan keamanan informasi yang merupakan *rate* yang dipengaruhi oleh beberapa biaya dan investasi seperti usaha pemulihan, usaha penilaian resiko, dan investasi pengelolaan keamanan informasi. Dimana investasi pengelolaan keamanan informasi merupakan gabungan dari tingkat investasi alat-alat keamanan dan tingkat investasi pencegahan serta ditambah dengan usaha pengurangan kerentanan. Selain beberapa stock dan rate yang terbentuk di dalam model juga terdapat beberapa variabel dan konstanta lain yang merupakan komponen input dari model pengelolaan keamanan informasi ini.

Model ini juga dilengkapi dengan formula-formula di setiap variabelnya untuk mendapatkan hasil analisa secara interaktif. Formula-formula tersebut dikelompokkan menjadi tiga bagian yaitu *Level/Stock*, *Input* (Konstanta), dan *Auxiliary*/Variabel. Dimana formula-formula tersebut adalah sebagai berikut.

1. *Stock*

Akumulasi Biaya Pengelolaan Keamanan Informasi= INTEG (Biaya Pengelolaan Keamanan Informasi, 0) (1)

Akumulasi Investasi Alat-alat Keamanan= INTEG (Tingkat Investasi Alat-alat Keamanan, 10000) (2)

Akumulasi Investasi Pencegahan= INTEG (Tingkat Investasi Pencegahan, 2000) (3)

Akumulasi Kerentanan= INTEG (Kerentanan Sistem, 0) (4)

Akumulasi Kerusakan= INTEG (Kerusakan-Usaha Pemulihan, 0) (5)

Akumulasi Laporan Serangan= INTEG (Laporan Serangan, 1) (6)

Total Serangan yang dapat dicegah= INTEG (Serangan yang dapat dicegah, 0) (7)

2. *Input*

Nilai Aset= 5000000 (8)

Image Organisasi= 0.5 pada skala [0,1] (9)

Investasi Alat-alat Keamanan= 5000 (10)

Investasi Pencegahan= 2000 (11)

Jumlah Penyerang= 100 (12)

Ketersediaan Alat-alat serangan= 0.5 pada skala [0,1] (13)

Motivasi Serangan= 0.5 pada skala [0,1] (14)

Nilai Target yang dirasakan= 0.5 pada skala [0,5] (15)

Start0= 0 (16)

Start1= 6 (17)

durasi0= 1 (18)

durasi1= 1 (19)

repeattime0= 12 (20)

repeattime1= 6 (21)

3. *Variabel*

Biaya Pengelolaan Keamanan Informasi= Investasi Pengelolaan Keamanan Informasi+Usaha Pemulihan*5+Usaha Penilaian Resiko*50 (22)

Dampak Pencegahan= 1-EXP(-1*0.125*Akumulasi Investasi Pencegahan/1000) pada skala [0,1] (23)

Daya tarik Target= 2.5*((Image Organisasi)/(Image Organisasi+1))*((Nilai Target yang dirasakan +0.2)/(Nilai Target yang dirasakan+0.5)) (24)

Investasi Pengelolaan Keamanan Informasi= Usaha Pengurangan Kerentanan*5+Tingkat Investasi Pencegahan+Tingkat Investasi Alat-alat Keamanan (25)

Jumlah Serangan= RANDOM UNIFORM(2.5*(Probabilitas Serangan*Jumlah Penyerang)*("Ketersediaan Alat-alat serangan" ^1.1), 7.5*(Probabilitas Serangan*Jumlah Penyerang)*("Ketersediaan Alat-alat serangan" ^1.1),0) (26)

Kelemahan Perangkat Lunak Dasar= 0.75*EXP(-0.01*Usaha Pengurangan Kerentanan) (27)

Kelemahan Perangkat Lunak Pengembangan= 0.5*EXP(-0.01*Usaha Pengurangan Kerentanan) (28)

Kemampuan Deteksi= 1-EXP(-0.001*"Akumulasi Investasi Alat-alat Keamanan"/5) (29)

Kerentanan Sistem= Resiko Keamamanan Perangkat Lunak*EXP(-2*Prosedur Keamaman) (30)

Kerentanan yang dirasakan= IF THEN ELSE(0.01*Akumulasi Kerentanan*Akumulasi Laporan Serangan<1,(0.01 *Akumulasi Laporan Serangan*Akumulasi Kerentanan),1) pada skala [0,1] (31)

Kerusakan= IF THEN ELSE(RANDOM UNIFORM(0,1,0)>0.5, 0.0002*Nilai Aset*Serangan Sukses *RANDOM EXPONENTIAL(0,1,0,1,0),0) (32)

Laporan Serangan= IF THEN ELSE(Serangan Sukses*Kerusakan*Mendekati Kerusakan=0,1,LN(Serangan Sukses)*(Kerusakan^Mendekati Kerusakan)/10) (33)

Mendekati Kerusakan= 1-EXP(-1*0.2*Serangan Sukses/10) (34)

Probabilitas Serangan= IF THEN ELSE((3.6*(0.1+(Kerentanan yang dirasakan-0.1)/(Kerentanan yang dirasakan +1))*(0.3+(Daya tarik Target-0.1)/(Daya tarik Target+0.5))*(0.1+(Motivasi Serangan-0.1)/(Motivasi Serangan+1))/Dampak Pencegahan)<1,(3.6*(0.1+(Kerentanan yang dirasakan-0.1)/(Kerentanan yang dirasakan+1))*(0.3+(Daya tarik Target-0.1)/(Daya tarik Target +0.5))*(0.1+(Motivasi Serangan-0.1)/(Motivasi Serangan+1))/Dampak Pencegahan),1) (35)

Prosedur Keamaman= 1-EXP(-0.5*Usaha Pengurangan Kerentanan/100) pada skala [0,1] (36)

Resiko Keamamanan Perangkat Lunak= 2.7*((Kelemahan Perangkat Lunak Pengembangan)/(Kelemahan Perangkat Lunak Pengembangan +1))*((Kelemahan Perangkat Lunak Dasar+0.1)/(Kelemahan Perangkat Lunak Dasar +0.5)) (37)

Serangan Sukses= ACTIVE INITIAL((1-Kemampuan Deteksi)*Jumlah Serangan,10) (38)

Serangan yang dapat dicegah= Kemampuan Deteksi*Jumlah Serangan (39)

"Tingkat Investasi Alat-alat Keamanan"= "Investasi Alat-alat Keamanan"*PULSE TRAIN(Start0,durasi0 , repeattime0 , FINAL TIME) (40)

Tingkat Investasi Pencegahan= Investasi Pencegahan*(PULSE TRAIN(Start1,durasi1,repeattime1,FINAL TIME)) (41)

Usaha Pemulihan= RANDOM UNIFORM(Kerusakan*0.5,Kerusakan*1.5,0) (42)

Usaha Pengurangan Kerentanan= RANDOM UNIFORM(Usaha Penilaian Resiko*0.5,Usaha Penilaian Resiko*1.5,0) (43)

Usaha Penilaian Resiko=
Kerusakan^Mendekati Kerusakan (44)

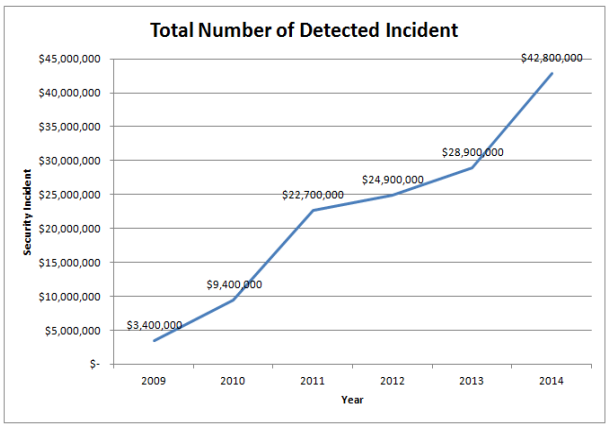
4.2. Verifikasi dan Validasi

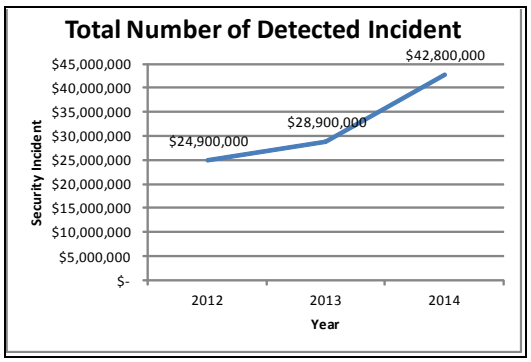
Validasi model sistem dinamik secara umum menggunakan dua pendekatan. Validasi struktur model untuk menentukan bahwa model menggambarkan sistem nyata secara akurat. Validasi perilaku model untuk memberikan tingkat kepercayaan terhadap hasil simulasi model sebelum di jalankan.

Validasi struktur dilakukan menggunakan verifikasi secara struktural dan analisis kondisi ekstrim. Verifikasi struktural menunjukkan apakah model konsisten dengan menggambarkan perilaku dunia nyata atau dengan literatur yang relevan. Struktur model pada penelitian ini dibangun berdasarkan model sistem dinamik untuk pengelolaan keamanan informasi, yang telah dibuat oleh Derek L. Nazareth, & Jae Choi (2014), dengan beberapa modifikasi dan memadukan struktur model pada penelitian lain yang di lakukan oleh Pei-Chen Sung dan Chien-Yuan Su (2013). Oleh karena itu model pada peneltian ini didasarkan pada literatur yang relevan sebagai persyaratan untuk membuat model sistem dinamik. Analisis kondisi ekstrim dilakukan untuk meyakinkan bahwa parameter-parameter di dalam model tidak berada pada kondisi yang ekstrim. Untuk mengukurnya perlu dilakukan pengamatan pada setiap variabel, apakah tingkah lakunya layak atau tidak dan konsisten secara logika. Apakah nilai dari setiap variabel melampau dari limit, misalkan probabiltas tidak kurang dari 0 dan tidak lebih dari 1. Misalkan pada variabel probabilitas serangan seperti diperlihatkan pada formula 35, formula pada variabel ini dibuat agar hasilnya tidak melebih limit antar 0 sampai dengan 1. Perlu diyakinkan bahwa seluruh parameter yang terlibat maksimal harus bernilai 1. Konstanta-konstanta dibuat untuk mendapatkan hasil yang tepat sehingga tidak melebihi angka 1.

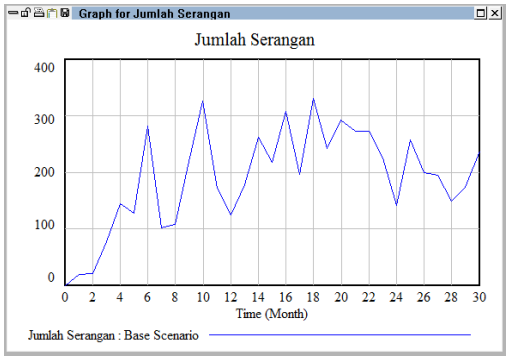
Validasi perilaku model menentukan bagaimana konsistensi *output* dari model apakah sesuai dengan perilaku dunia nyata. Salah satu contoh kasus kita ambil pada jumlah insiden yang terjadi pada suatu survey. Insiden yang dilaporkan oleh responden *The Global State of Information Security Survey* 2015 terus naik dari tahun ke tahun. Survei tahunan lebih dari 9.700 keamanan, IT, dan eksekutif bisnis menemukan bahwa jumlah insiden keamanan terdeteksi oleh responden naik menjadi 42,8 juta pada tahun 2014, meningkat 48% dari tahun 2013. Itu setara dengan 117.339 serangan masuk per hari. Dari data survei menunjukkan bahwa *the Coumpound Anual Rate* (CAGR) dari insiden keamanan terdeteksi telah meningkat 66% dari tahun ke tahun sejak tahun 2009 (www.pwc.com/gsiss2015, 2015 : 7).

Pada hasil survai yang ditunjukkan pada gmabr 4.1 mengambarkan insiden keamanan yang terjadi dari tahun ke tahun, sedangkan model simulasi sistem dinamik yang dibuat pada penelitian ini mengambarkan perilaku dalam periode selama 30 bulan berarti bisa kita konversikan ke dalam tahun menjadi 2,5 tahun. Maka paling tidak kita bisa mengamati dari 3 tahun terakhir dari hasil survai. Hasilnya seperti dilihat pada gambar 4.2 yang dibandingan dengan hasil model simulasi pada jumlah serangan yang terjadi. Pada gambar tersebut dapat diamati bahwa perilaku dalam periode waktu tertentu antara model simulasi dengan sistem aktual memiliki tren yang sama. Hal ini menandakan model simulasi telah menggambarkan sistem real yang diamati. Selanjutnya model sistem simulasi tersebut dapat digunakan untuk menjalankan berbagai skenario pengujian.





Gambar 4.1. Total Jumlah Insiden Keamanan Dilaporkan Oleh Responden *The Global State of Information Security Survey* 2015



Gambar 4.2. Perbandingan Perilaku Dalam Periode 3 Tahun Terakhir Hasil Survey Insiden Serangan dengan

Periode 30 bulan (2.5 Tahun) Jumlah Serangan Pada Model Simulasi

Tabel 4.1. Penentuan Variabel Pengungkit (*leverage*)

No	Variabel	Loops	Rangking	Ketera-ngan
1	Akumulasi Laporan Serangan	3	4	
2	Akumulasi kerentanan system	6	2	
3	Laporan serangan	3	4	
4	Kerentanan system	6	2	
5	Kerusakan	4	3	
6	Jumlah Serangan	9	1	
7	Probabilitas serangan	9	1	
8	Serangan sukses	9	1	
9	Mendekati Kerusakan	4	3	
10	Kerentanan yang dirasakan	9	1	Leverage
11	Prosedur keamanan	2	5	
12	Usaha pengurangan kerentanan	6	2	
13	Resiko keamanan perangkat lunak	4	3	
14	Usaha Penilaian Resiko	6	2	
15	Kelemahan perangkat lunak dasar	2	5	
16	Kelemahan perangkat lunak pengembangan	2	5	

1. Skenario Dasar

Model simulasi sistem dinamik pengelolaan keamanan informasi yang telah dibuat, divalidasi dan diverifikasi kemudian dapat digunakan sebagai alat untuk melakukan simulasi perubahan kebijakan. Untuk memperlihatkan perilaku setiap variabel yang terlibat dalam jangka waktu tertentu, model ini disimulasikan dengan unit periode waktu bulan yaitu selama 30 bulan. Untuk memperlihatkan hasil yang terbaik perlu dilakukan simulasi dalam berbagai kondisi untuk mengetahui dampak dari setiap perbedaan kebijakan keamanan informasi, yaitu dengan cara melakukan perubahan-perubahan nilai pada setiap variabel input pada model yang mempengaruhi seluruh variabel di dalam sistem.

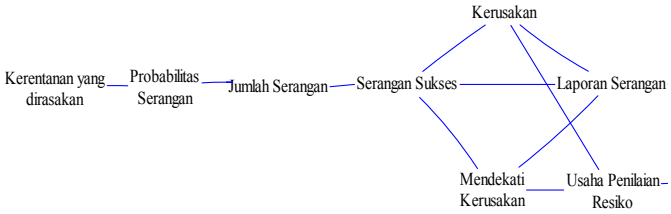
Skenario dasar perlu ditentukan terlebih dahulu. Dalam model ini nilai aset ditentukan sebesar $5.000.000, dengan jumlah populasi penyerang 100, ditambah dengan investasi alat-alat keamanan sebesar $5.000 yang dilakukan investasi setiap satu tahun sekali dan investasi pencegahan sebesar $2.000 yang dilakukan investasi setiap enam bulan sekali.

2. Penentuan Variabel Pengungkit (Leverage)

Untuk menentukan variabel *leverage* langkah pertama adalah memperhatikan variabel-variabel yang bersinggungan langsung dengan loop, kemudian menghitungnya. Setelah dihitung kemudian dilakukan perangkingan untuk mencari variabel dengan jumlah *loop* terbanyak.

Setelah dilakukan pengamatan dan penghitungan maka didapatkan hasil yang terlihat pada tabel 4.1.

Tampak terdapat variabel dengan nilai loop terbanyak 9 loop dimana ada 4 variabel yaitu, Jumlah Serangan, Probablitas Serangan, Serangan Sukses, dan Kerentanan yang dirasakan. Karena terdapat 4 variabel dengan nilai yang sama maka perlu diamati variabel mana yang merupakan variabel yang paling berpengaruh di dalam loop, dengan mengamati struktur loop maka didapatkan bahwa kerentanan yang dirasakan merupakan variabel yang paling berpengaruh di dalam loop karena variabel ini berada pada posisi paling awal dan mempengaruhi probabilitas serangan, jumlah serangan dan serangan sukses. Gambar 4.3 memperlihatkan *uses tree* dari kerentanan yang dirasakan dimana posisi variabel ini berada pada posisi paling awal pada *loop*.



Gambar 4.3. *Uses Tree* Kerentantan yang dirasakan sebagai variabel *Leverage*

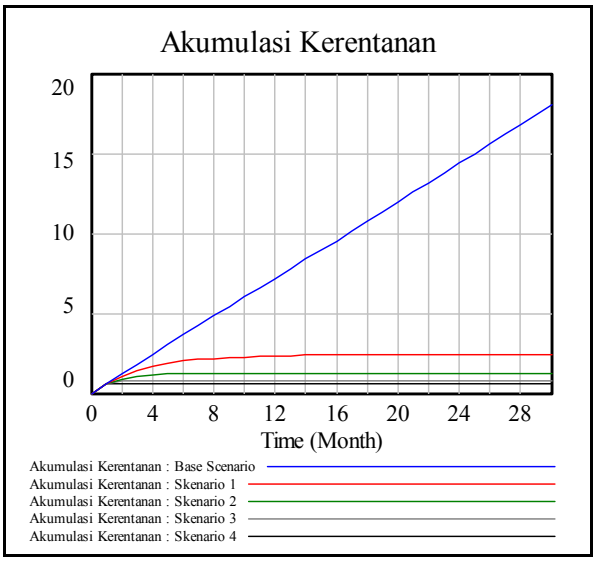
3. Simulasi Perubahan Kebijakan

Dalam simulasi ini terdapat beberapa variabel yang merupakan variabel yang nilainya bisa ditentukan melalui kebijakan organisasi. Untuk menentukan variabel mana saja yang sangat berpengaruh pada hasil simulasi, perlu dilakukan pengamatan pada setiap variabel. Sebelumnya telah dilakukan analisa untuk menentukan variabel pengungkit (*leverage*) dan analisa tersebut menghasilkan bahwa kerentanan yang dirasakan adalah merupakan variabel sensintif yang paling banyak bersinggungan dengan loop. Pada model simulasi ini juga akan dilakukan simulasi untuk memperlihatkan pengaruh yang terjadi apabila dilakukan perubahan nilai pada variabel tersebut.

Setelah model yang dibangun dirasa sudah sesuai dengan harapan baik secara struktural maupun perilakunya, maka model ini dapat digunakan untuk menginvestigasi dampak dari perubahan nilai kerentanan dengan memanipulasi nilai pada probabiltas pengurangan kerentanan. Nilai probabilitas pengurangan kerentanan akan dibuat menjadi bervariasi dari mulai 0 sampai dengan 1 dengan interval 0.25. Akumulasi kerentanan, Akumulasi laporan serangan, kerusakan dan biaya pengelolaan keamanan informasi hasilnya dapat diketahui setelah dilakukan simulasi dengan nilai probabiltas kerentanan yang berbeda, yang tampak pada tabel 4.2.

Tampak pada tabel 4.2 bahwa seluruh tren pada hasil simulasi sudah cukup untuk bisa diprediksi. Angka-angka ini dadapatkan dari model simulasi, dan akumulasi yang diambil adalah setelah akhir periode simulasi yaitu 30 bulan. Berdasarkan tingkat probabilitas pengurangan kerentanan untuk setiap skenario menunjukkan bahwa semakin besar probabiltas pengurangan kerentanan maka akumulasi kerentanan semakin berkurang, akumulasi laporan serangan semakin berkurang, akumulasi kerusakan semakin berkurang, demikian pula dengan akumulasi biaya pengelolaan keamanan informasi juga semakin berkurang. Dengan demikian hasil simulasi memperlihatkan perubahan nilai pada variabel-variabel yang terlibat di dalam *loop* setelah dilakukan perubahan nilai pada variabel *leverage.*

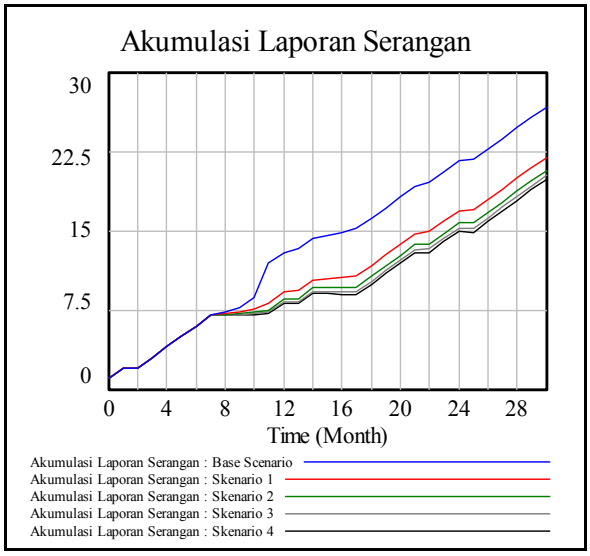
Hasil simulasi dalam bentuk tabel telihat belum cukup untuk menggambarkan perilaku model, maka perlu digambarkan dalam bentuk grafik. Penggambaran dalam bentuk grafik akan lebih mudah dipahami, karena perubahan nilai dan perilaku model dapat terlihat secara visual, sehingga memudahkan untuk mengamati hasil simulasi. Pengambaran perilaku dalam bentuk grafik dapat dilihat pada gambar 4.4 sampai dengan gambar 4.7. Tampak pada gambar-gambar tersebut menggambarkan tren dari empat variabel yaitu akumulasi kerentanan, akumulasi laporan serangan, akumulasi kerusakan dan akumulasi biaya pengelolaan keamanan informasi dengan perubahan untuk setiap tingkat skenario probabilitas pengurangan kerentanan.



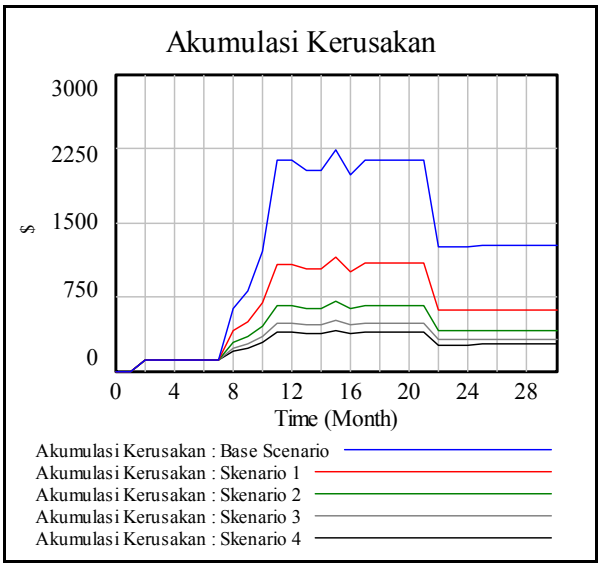
Gambar 4.4. Akumulasi Kerentanan menggunakan Perbedaan Probabilitas Pengurangan Kerentanan

Tabel 4.2. Hasil Simulasi untuk Probabilitas Pengurangan Kerentanan

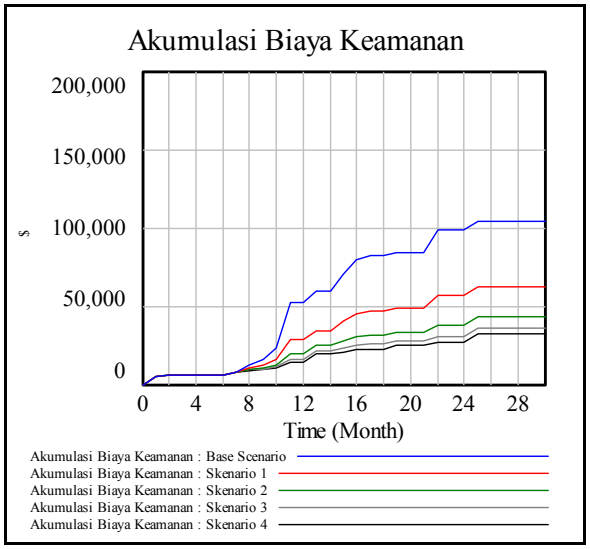
Scenario	Probabilitas Pengurangan Kerentanan	Akumulasi Kerentanan	Akumulasi Laporan Serangan	Akumulasi Kerusakan ($)	Akumulasi Biaya Pengelolaan Keamanan Informasi ($)
Base Scenario	0	18.04	26.72	1269	104,300
Scenario 1	0.25	2.442	21.95	622.4	61,820
Scenario 2	0.5	1.224	20.73	414.9	43,020
Scenario 3	0.75	0.816	20.19	317.4	35,700
Scenario 4	1	0.612	19.86	267.4	31,940



Gambar 4.5. Akumulasi Laporan Serangan menggunakan Perbedaan Probabilitas Pengurangan Kerentanan



Gambar 4.6. Akumulasi Kerusakan menggunakan Perbedaan Probabilitas Pengurangan Kerentanan



Gambar 4.7. Akumulasi biaya pengelolaan keamanan informasi menggunakan Perbedaan Probabilitas Pengurangan Kerentanan

Pada grafik akumulasi kerentanan terlihat bahwa skenario dasar memperlihatkan suatu penguatan, terlihat bahwa tanpa adanya perngurangan kerentanan atau dengan probabilitas 0 maka kurvanya semakin menguat atau linier. Setelah ada pengurangan kerentanan dengan probabilitas yang sedikit-demi sedikit dinaikkan maka terlihat kurvanya semakin menurun dan membentuk garis lurus datar, artinya menunjukkan suatu keseimbangan atau *goal seeking*. Grafik yang lain seperti akumulasi serangan juga memperlihatkan tren menurun, sehingga dengan menurunnya serangan maka akumulasi kerusakan dan akumulasi biaya pengelolaan keamanan informasi juga memperlihatkan kurva yang semakin menurun. Akan tetapi bisa di perhatikan bahwa terdapat sedikit perbedahan pada akumulasi kerusakan, grafiknya naik kemudian turun, penurunan yang terjadi dikarenan bahwa akumulasi kerusakan juga akan berkurang akibat adanya usaha pemulihan sehingga akumulasi kerusakan ini tidak selalu naik tetapi ada keseimbangan disini.

Kebijakan yang dibuat dengan merubah nilai probablitas pengurangan kerentanan memperlihatkan pengaruh yang signifikan pada model, sehingga menjadikan kerentanan yang dirasakan merupakan variabel input yang sangat penting dalam pengelolaan keamanan. Perngaruhnya terhadap akumulasi kerentanan langsung dapat dirasakan dan tampak jelas pada awal perubahan nilai probabilitas.

4. Implikasi Penelitian Pemodelan Sistem Dinamik

Secara mendasar model simulasi sistem dinamik pengelolaan keamanan informasi telah memberikan panduan yang jelas kepada manager dalam hal pengelolaan investasi dan biaya keamanan informasi. Penentuan variabel pengungkit yaitu kerentanan yang dirasakan

menunjukkan titik permasalahan yang memberikan pengaruh besar dari pengelolaan keamanan infomasi. Dengan membuatkan alternatif solusi untuk pengelolaan kerentanan ini, membuat manager memiliki kewaspadaan dalam mengambil keputusan untuk melindungi aset keamanan informasi organisasi.

Di dalam model sistem dinamik pengelolaan keamanan informasi memberikan gambaran bahwa perbedaan usaha dalam pengelolaan resiko dengan memberikan tingkat probabilitas pengurangan kerentanan memiliki implikasi yang berbeda terhadap keseluruhan biaya yang harus dikeluarkan untuk pengelolaan aset keamanan informasi. Hal yang paling mendasar adalah setiap ada kenaikan tingkat probabilitas pengurangan kerentanan maka seluruh biaya pengelolaan keamanan informasi akan terjadi penurunan. Pengurangan kerentanan keamanan informasi berdampak kepada seluruh variabel yang ada. Untuk mendeteksi kerentanan sistem dapat dilakukan secara manual akan tetapi hal ini akan menyita banyak waktu, karena membutuhkan sumber daya manusia yang secara langsung melakukan pemeriksaan dengan memadankan sistem dengan informasi kerentanan yang didapat. Untuk itu, teknologi keamanan seperti *Vulnerability Scanner* dan *Intrusion Detection System* berperan dalam mempercepat proses ini. Oleh karena itu pengurangan kerentanan juga dipengeruhi oleh investasi pencegahan dan alat alat deteksi keamanan informasi, sehingga implikasinya jelas bahwa manajer keamanan informasi harus memperhatikan pengelolaan variabel-variabel tersebut.

Terdapat beberapa implikasi pada penelitian ini. Peneltian ini mengembangkan model simulasi sistem dinamik yang dapat digunakan untuk mengeksplorasi dan mengetahui implikasi dari perbedaan usaha dalam pengelolaan resiko dengan memberikan tingkat probabilitas pengurangan kerentanan sehingga dapat diambil keputusan pengelolaan keamanan informasi dengan memberikan nilai investasi yang tepat. Model ini juga dapat digunakan untuk menginvestigasi keamanan informasi di bawah berbagai kondisi. Sebagai contoh, jika organisasi merupakan target yang menarik untuk diserang, maka jumlah serangan akan semakin meningkat. Serangan baru keamanan informasi selalu berkembang dan semakin canggih sehingga semakin meningkatkan serangan sukses yang terjadi. Ini memperlihatkan bahwa seluruh perubahan yang diberikan kepada variabel input di dalam model akan mempengaruhi variabel lain yang menerima inputan tersebut. Dengan demikian bahwa kebutuhan akan eksplorasi yang sistematik pada lingkup penelitian dan analisis struktur yang detail untuk meyakinkan bahwa variabel-variabel yang terdapat di dalam model memiliki perilaku yang tepat.

V. KESIMPULAN

Bentuk model simulasi komputer pemodelan sistem dinamik untuk menganalisis strategi kebijakan dalam pengelolaan keamanan informasi mempunyai beberapa skenario yang terbagi dalam beberapa model yaitu.

1. Model Serangan, model yang menjelaskan hubungan sebab-akibat antar variabel yang menunjukkan bagaimana terjadinya serangan, yang merupakan *loop* yang semakin menguat, sehingga serangan sukses yang terjadi menyebabkan peningkatan laporan serangan.
2. Model Kerentanan, model ini muncul akibat dari *loop* serangan yang merupakan hubungan sebab-akibat antar variabel yang menunjukkan kerentanan yang dirasakan. Ini adalah *loop* balancing dan cenderung akan mencari keseimbangan dan akan mempengaruhi *loop* penguatan pada serangan.
3. Model biaya pengelolaan keamanan informasi, merupakan model yang menunjukkan keseluruhan biaya yang dikeluarkan yang menghasilkan *output* berupa akumulasi biaya pengelolaan keamanan informasi, baik yang berasal dari investasi maupun biaya yang ditimbulkan dalam usaha-usaha pengelolaan keamanan informasi.

Hasil simulasi komputer untuk pemodelan sistem dinamik dengan melakukan perubahan kebijakan melalui probabilitas pengurangan kerentanan dengan mengubah nilainya menjadi 0, 0.25, 0.5, 0.75 dan 1 yang mempunyai arti bahwa kerentanan sistem yang dirasakan perlu dilakukan pengurangan dengan cara menutupi kerentanan-kerentanan tersebut. Dimana untuk melakukan itu perlu dilakukan usaha yang diukur sesuai dengan tingkat kemungkinan kerentanan yang dapat ditutupi. Melalui pengamatan empat variabel akumulasi dihasilkan nilai penurunan pada setiap tingkat perubahan skenario kebijakan, yang menunjukkan arti bahwa semakin besar tingkat kemungkinan kerentanan yang berhasil ditutupi akan menekan akumulasi kerentanan, laporan serangan, kerusakan dan biaya pengelolaan keamanan informasi.

Refernsi

[1] Ae Chan Kim, Su Mi Lee, Dong Hoon Lee, "*Compliance Risk Measures of Financial Information Security using System Dinamics*", *International Journal of Security and its Applications*, Vol. 6, No. 4, Oktober, 2012, pp: 191-200.

[2] Abbas, H., Magnusson, C., Yngstrom, L., dan Hemani, A., "*Addressing Dynamic Issues in Information Security Management*", *International Journal of Information Management & Computer Security*, Vol. 19 No. 1, 2011, pp 5-24.

[3] Deborah Marshall, Paul Rogers, Thomas Rohleder, Sonia Vanderby, "*System Dynamic Modelling: A Decission Support Tool to Improve Care for HIP & Knee Oesteoarthritis*", Alberta Canada: Institut of Health Economic, 2010.

[4] Derek L. Nazareth, Jae Choi, "*A System Dynamics Model for Information Security Management*" *International Journal of Information & Management*, 52 (2015) 123-134.

[5] Dr Mike Yearworth, "*A Brief Interoduction to System Dynamics Modelling*" University of Bristol, 2014.

[6] Eric Pruyt, "*Small System Dynamics Models for Big Issues*", TU Delft Library, Delft, The Netherlands, 2013.

[7] Erma Suryani, Shou-Yan Chou, Rudi Hartono, Chin-Hsien Chen, "*Demand Secenario Analysis and Planned Capacity Expantion: A System Dynamic Framework*", *International Journal of Simulating Modelling Practice and Theory*, 18 (2010) 732-751.

[8] John Hayward, Graeme P. Boswell, "*Model Behavior and the Concept of Loop Impact: A Practical Method*", *Sistem Dinamik Society*, Vol. 30, No. 1-2, (January-June 2014): 29-57, doi: 10.1002/sdr.1551

[9] http://vensim.com, diakses pada tanggal 10 Mei 2015.

[10] Kljajić, M., Boršnar, M.K., Škraba, A., Kofjač, D., "*Sistem Approach to MIS and DSS and its Modeling within SD*", IGI Global, 315-335. doi: 10.4018/978-1-4666-0882-5,ch2.8.

[11] Liu Wei, Cui Yong-feng, Li Ya, "*Information System Security Assessment Based on System Dynamics*", *International Journal of Security and its Applications* (IJSIA), Vol. 9, No. 2 (2015), pp. 73-84.

[12] Oxa Axella, Erma Suryani, "Aplikasi Model Sistem Dinamik untuk Menganalisis Permintaan dan Ketersediaan Listrik Sektor Industri (Studi Kasus: Jawa Timur)", Jurnal Teknik ITS Vol. 1, (Sept, 2012) ISSN: 2301-9271.

[13] Pei-Chen Sung, Chien-Yuan Su, "*Using System Dynamics to Investigate the Effect of the Information Medium Contact Policy on the Information Security Management*", International Journal of Business and Management Vol 8, 12 (2013) 1833-3850.

[14] Yang, S., Wang, Y., "*System Dynamic Based Insider Threats Modeling*", International Journal of Network Security & Its Aplication (IJNSA), vol. 3, No. 3, May 2011, doi: 10.5121/ijnsa.2011.3301.