STUDI MODEL ORGANISASI CSIRTs (*COMPUTER SECURITY INCIDENT RESPONSE TEAMS*) PADA PERUSAHAAN BERSKALA BESAR

Riza Kurniawan, Budi Rahardjo
Laboratorium Sistem Kendali dan Komputer (LSKK), KK Teknologi Informasi
Jln. Ganesha 10, Labtek VIII Lt. 2, Sekolah Teknik Elektro dan Informatika (STEI) ITB, Bandung
e-mail: mail2riza@gmail.com, rahard@gmail.com

ABSTRAKSI

Kebutuhan akan keamanan sistem informasi merupakan hal yang sangat penting bagi suatu perusahaan dalam menjamin kesuksesan proses bisnisnya. Hal ini mempunyai hubungan yang signifikan apabila dikaitkan dengan meningkatkannya jumlah insiden keamanan komputer serta kerugian yang ditimbulkannya. Dewasa ini, konsep keamanan yang merupakan sebuah proses manajemen yang berkelanjutan dan melibatkan seluruh komponen dari suatu perusahaan, telah meninggalkan cara konvensional yang hanya mengandalkan keamanan pada kemampuan perangkat lunak atau perangkat keras. Salah satu alternatif solusi manajemen keamanan tersebut adalah dengan membentuk CSIRTs (Computer Security Incident Response Teams) pada organisasi atau perusahaan. Penelitian tentang Model Organisasi CSIRTs telah dirintis oleh CMU/SEI (Carnegie Mellon University/Software Engineering Institute) sejak tahun 1998. Pada tesis ini, akan dilakukan suatu studi kelayakan salah satu model organisasi CSIRTs tersebut, yang disegmentasikan pada perusahaan berskala besar. Studi ini, akan menggunakan metoda CBA (Cost Benefit Analysis) untuk pengujian dari sisi ekonomi, dan CMMI (Capability Maturity Model Integration) dari sisi manajemen.

Kata kunci: *keamanan sistem informasi, CSIRTs, Model Organisasi CSIRTs, perusahaan berskala besar, CBA, CMMI.*

1. PENDAHULUAN

Berdasarkan laporan *Computer Emergency Response Team Coordination Center* (CERT/CC)[7] tentang insiden keamanan komputer, tercatat sebanyak 319.992 insiden terjadi di dunia selama tahun 1988-2003. sedangkan di Indonesia, berdasarkan laporan APJII[12] (Asosiasi Penyedia Jasa Internet Indonesia) tentang insiden dan penyalahgunaan komputer, tercatat kira-kira 33.843 insiden yang terjadi pada tahun 2002-2003.

Sedangkan di Indonesia, untuk merespon isu tentang insiden keamanan komputer tersebut, pada bulan oktober 2006 pemerintah sedang merancang suatu tim yang disebut *Indonesia-Security Incident Response Team on Internet Infrastructure* (ID-SIRTII). Pembentukan tim yang berlandaskan Peraturan Menteri Komunikasi dan Informatika Nomor 27 tahun 2006[9] ini, memiliki tujuan melakukan usaha-usaha pengamanan atas pemanfaatan jaringan telekomunikasi berbasis protokol internet di Indonesia.

Di sisi lain, yaitu pada perusahaan-perusahaan di Indonesia, kebutuhan adanya CSIRTs akan sangat menentukan bagi keamanan informasi usahanya. Sesuai dengan skala usahanya, jika terjadi suatu insiden pada perusahaan-perusahaan tersebut, maka yang akan menderita kerugian cukup besar adalah perusahaan dengan kategori berskala besar. Sehingga kehadiran tim penanganan insiden keamanan komputer ini, seharusnya segera diimplementasikan pada perusahaan tersebut.

Penelitian tentang bentuk model organisasi CSIRTs telah dilakukan oleh Carnegie Mellon University/Software Engineering Institute (CMU/SEI)[5] sejak tahun 1998. berdasarkan survei yang dilakukan oleh CERT CSIRTs Development Teams[6], terdapat satu model organisasi CSIRTs yang umumnya sering diimplementasikan pada organisasi berskala besar, yaitu *Internal Centralized* CSIRTs. Pada penelitian ini akan dibahas suatu studi dari penerapan konsep model organisasi CSIRTs tersebut pada perusahaan generik berskala besar.

2. PERUMUSAN MASALAH

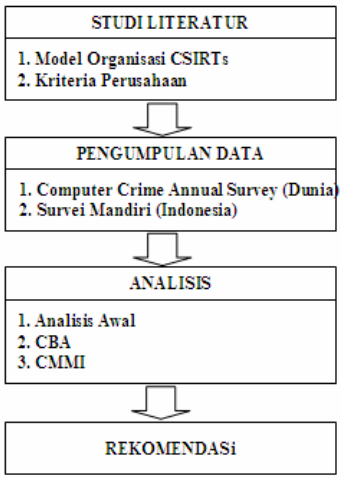
Permasalahan yang akan dibahas dalam penelitian ini adalah, melakukan suatu studi kelayakan untuk menentukan bentuk model organisasi CSIRTs yang sesuai pada perusahaan generik berskala besar di Indonesia.

3. TUJUAN PENELITIAN

a. menentukan bentuk model organisasi CSIRTs yang sesuai (*feasible*) untuk diimplementasikan pada perusahaan generik berskala besar di Indonesia;
b. menguji salah satu contoh prosedur layanan organisasi CSIRTs, untuk menentukan bahwa model organsasi CSIRTs tersebut akan sesuai jika diimplementasikan pada perusahaan generik berskala besar di Indonesia;
c. memberikan rekomendasi dalam pengimplementasian model organisasi CSIRTs pada perusahaan berskala besar di Indonesia.

4. METODOLOGI PENELITIAN

Dalam Gambar 1 merupakan gambaran proses metodologi yang dilakukan akan dilakukan pada penelitian ini.



Gambar 1. Proses metodologi penelitian

5. INSIDEN KEAMANAN KOMPUTER

Menurut Jimmy Arvidsson[3], taksonomi terminologi insiden keamanan komputer terdiri dari:

a. serangan (*attack*)
suatu serangan pada keamanan informasi yang dilakukan dengan sengaja dan berasal dari ancaman terencana dengan teknik atau metoda tertentu. Serangan ini ditujukan untuk mengelabui atau merusak sistem, baik secara pasif atau aktif, dari luar ataupun dari dalam sistem, atau dengan perantara;

b. penyerang (*attacker*)
adalah individu atau kelompok yang berusaha melakukan satu atau beberapa serangan pada sistem informasi untuk mencapai tujuannya;

c. target
adalah sistem komputer atau jaringannya, dapat berupa entitas logika (rekening, proses, data) atau entitas fisik (komponen dari komputer, jaringan, atau (*internetwork*);

d. korban (*victim*)
adalah individu atau organisasi yang menderita akibat insiden yang dapat diketahui dari laporannya insiden;

e. kelemahan (*vulnerabiliy*)
Suatu kelemahan atau kekurangan dalam suatu disain sistem, implementasi, manajemen dan operasional, yang bisa dimanfaatkan untuk melanggar kebijakan keamanan sistem;

f. bukti (*evidence*)
adalah informasi yang berkenaan dengan suatu peristiwa yang membuktikan atau mendukung suatu kesimpulan tentang fakta yang telah terjadi;

g. kejadian (*event*)
Suatu aksi yang mengarah pada suatu target dimana diharapkan dapat mengakibatkan suatu perubahan status pada target;

h. insiden (*incident*)
adalah suatu peristiwa yang mungkin dapat menjurus pada dampak yang serius, krisis, atau bencana;

i. insiden keamanan komputer (*computer security incident*)
suatu hal yang riil, yang melanggar hukum atau otorisasi atau yang tidak diperbolehkan, sehubungan dengan sistem komputer atau sistem jaringan;

6. KRITERIA PERUSAHAAN BERSKALA BESAR DI INDONESIA

Beberapa kriteria berkaitan dengan skalabilitas usaha di Indonesia yang dirangkum dari beberapa sumber, maka dapat diasumsikan, kriteria perusahaan berskala besar di Indonesia adalah:

1) untuk sektor industri, memiliki total aset lebih dari Rp. 5 miliar dan untuk non industri, memiliki kekayaan bersih lebih dari Rp. 600 juta[8];
2) unit kegiatan yang memiliki kekayaan bersih lebih besar dari Rp. 200 juta s.d. maksimal 10 miliar (tidak termasuk tanah & bangunan untuk usaha) [8];
3) memiliki pekerja di atas 2000 orang[8].

7. KONSEP ORGANISASI CSIRTS

a. Definisi CSIRT

Secara umum, CSIRTS dapat didefinisikan sebagai, *suatu organisasi atau tim yang menyediakan pelayanan dalam mencegah, menanggulangi dan menanggapi insiden keamanan komputer, pada suatu wilayah tanggung jawab* (*constituency*) *tertentu*[9].

b. Jenis model organisasi CSIRTS

Berdasarkan konsep Carnegie Mellon University/Software Engineer Institute (CMU/SEI), terdapat lima model organisasi CSIRTS[5] yaitu:

1) *Security Team*
Pada model ini tidak ada tim CSIRT yang dibentuk untuk menangani insiden. Model ini hanya mengandalkan sumber daya yang ada (misalnya staf pada departemen TI) untuk menangani insiden keamanan yang terjadi pada organisasi induk;
2) *Internal Distributed* CSIRTS
Adalah model tim yang terdistribusi dan tersebar pada organisasi atau letak geografis. Pada tim ini terdapat seorang manajer yang berusaha mengkoordinasikan tim-tim yang terdistribusi tersebut. Secara umum tim ini bekerja secara paruh waktu (*part time*);
3) *Internal Centralized* CSIRTS
Model tim ini terletak terpusat secara fisik dan geografis pada organisasi induk. Tim ini menyediakan layanan penanganan insiden bagi unit organisasi induk atau *constituency*-nya; Secara umum tim ini bekerja secara penuh (*dedicated*);
4) *Internal Combined Distributed and Centralized* CSIRTS

Model ini merupakan kombinasi dari *internal distributed* dan internal *centralized*. Umumnya tim *internal distributed* terletak pada cabang organisasi dan berkoordinasi dengan *internal centralized* yang berada pada pusat organisasi;

5) *Coordinating* CSIRTS;
Model ini umumnya terletak terpusat pada organisasi induk. Tujuan dari tim ini berusaha mengkoordinasikan tim-tim CSIRTS lain, yang berada dalam *constituency*-nya.

c. *CSIRTS framework*[9]

Untuk mencapai tujuannya, CSIRTS memiliki kerangka kerja sebagai berikut:

1) Pendeklarasian Misi
Pada bagian ini, tim CSIRT yang akan dibentuk harus dapat mendefinisikan dengan jelas misi yang akan dijalankan, dalam bentuk tujuan umum, sasaran dan prioritas;
2) *constituency*
merupakan wilayah kerja atau yuridiksi dari tim CSIRTS. Berikut ini merupakan pembagian dari *constituency* dan relasinya pada entitas internal ataupun eksternal pada perusahaan,

Tabel 1. *constituency* CSIRTS dan misinya

Model CSIRTS	***Misi***	***constituency***
Coordinating CSIRTS	Membangun suatu pengetahuan dasar (*knowledge base*) dalam perspektif global keamanan komputer dan membina kerjasama dengan tim CSIRTS lain di dunia	Meliputi suatu negara atau dengan tim CSIRTS lain di dunia
CSIRT internal perusahaan (*Internal Distributed* CSIRTS, *Internal Centralized* CSIRTS dan kombinasi-nya)	Meningkatkan keamanan sistem informasi di perusahaan dan memperkecil efek dari insiden keamanan yang terjadi	
Security Teams	Meningkatkan keamanan sistem informasi pada perusahaan dengan menggunakan sumber daya yang ada	Penguna layanan keamanan sistem informasi

Sedangkan berdasarkan otoritasnya, model organisasi CSIRTS memiliki tiga tipe otoritas yang berhubungan dengan *constituency*-nya. Di bawah ini adalah tipe otoritas organisasi CSIRTS tersebut,

Tabel 2. *constituency* CSIRTS dan otoritasnya

Tingkatan otoritas	Relasi *constituency*
penuh (*full*)	Tim CSIRTS memiliki otoritas penuh dalam menjalankan tugas sesuai *constituency* nya.
berbagi (*shared*)	Tim CSIRTS berusaha mendukung proses keamanan sistem informasi pada perusahaan atau organisasi. Serta ikut serta dalam proses pengambilan keputusan mengenai *constituency* nya.
tidak ada otoritas *(none*)	Tim CSIRTS hanya memberikan rekomendasi mengenai *constituency* nya dan tidak berperan aktif dalam pengambilan keputusan.

d. Jenis-jenis pelayanan CSIRTS[5]

Secara umum suatu tim CSIRTS harus memiliki tiga jenis pelayanan terhadap *constituency* nya, antara lain,

1) Pelayanan Reaktif (*Reactive Services*)
Pelayanan ini merupakan pelayanan dasar yang harus disediakan oleh CSIRTS. Pelayanan ini dapat dipicu oleh suatu kejadian atau berdasarkan permintaan. Sebagai contoh, jika terdapat penyebaran kode program yang berbahaya, jika ada laporan kelemahan pada perangkat lunak (*software vulnerabilities*), atau adanya permintaan dari organisasi induk atau tim CSIRTS lainnya;
2) Pelayanan Proaktif (*Proactive Services*)
Pelayanan ini menyediakan panduan dan informasi untuk mempersiapkan, melindungi, dan mengamankan sistem *constituency*-nya, dalam mengantispasi serangan, masalah, atau insiden keamanan komputer. Performa pelayanan ini akan mereduksi permasalahan insiden di masa mendatang;
3) Pelayanan Manajemen Kualitas Layanan Keamanan (*Service Security Quality Manajemen Service*).

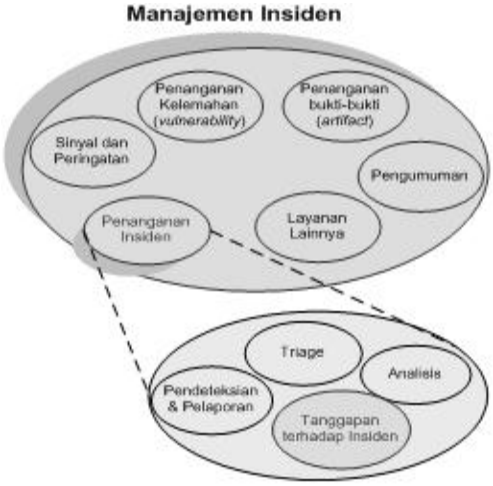
Pelayanan ini ditujukan untuk meningkatkan kualitas dari pelayanan keamanan yang dilakukan oleh bagian lain pada organisasi induk, misalnya, departemen IT (*Information Technology*) atau Divisi Keamanan (*security division*).

e. Manajemen insiden dan penanganan insiden

Adalah seluruh proses operasional yang tercakup pada layanan CSIRTS, pada proses ini terdapat *sub* proses penanganan insiden yang umumnya meliputi beberapa fungsi yaitu:

1) pendeteksian dan pelaporan
kemampuan untuk menerima dan menganalisis laporan, kejadian, atau permintaan penanganan insiden[2];
2) *triage*
adalah proses operasional untuk melakukan pengurutan (*sorting*), pengkategorian, dan pemberian prioritas terhadap laporan dan kejadian dari setiap insiden[2];
3) analisis
adalah proses untuk mendapatkan informasi yang lebih akurat tentang insiden yang terjadi, dampak terhadap *constituency*, dan metoda atau langkah pemulihan yang harus diambil[2];
4) tanggapan terhadap insiden
adalah proses opersional yang dilakukan dalam melakukan metoda atau langkah pemulihan yang harus diambil berkaitan dengan insiden[2].

Gambar 2 adalah gambaran umum proses tersebut pada CSIRTS.



Gambar 2. Manajemen & penanganan insiden

8. ANALISIS KELAYAKAN MODEL ORGANISASI CSIRTS PADA PERUSAHAAN BERSKALA BESAR

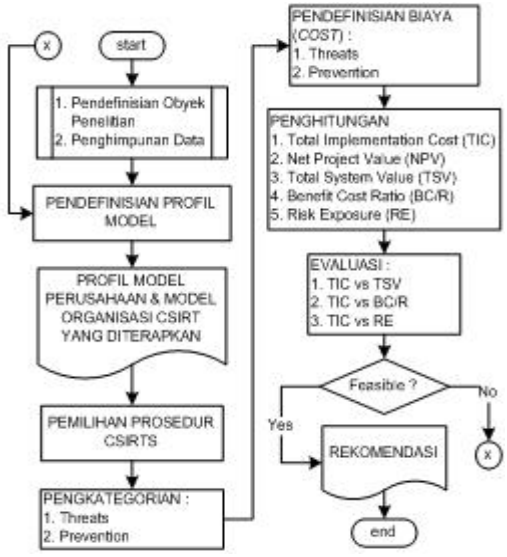
Pada penelitian ini akan dilakukan beberapa analisis yaitu:

a. Analisis Awal

Proses ini adalah untuk menentukan obyek model organisasi CSIRTS yang akan diteliti. Hasil dari proses ini akan berupa model perusahaan generik skala besar yang akan mengimplementasikan salah satu model organisasi CSIRTS, yaitu model Internal Centralized CSIRTS.

b. *Cost Benefit Analysis* (CBA)

Secara umum CBA didefinisikan sebagai *sebuah pendekatan dengan skala pertimbangan* (*weighing-scale*) *dalam pengambilan keputusan*[10]. Tujuan CBA pada penelitian ini adalah untuk memberikan masukan terbaik terhadap kebijakan pembentukan CSIRTS pada suatu model perusahaan generik berskala besar. Gambar 3 adalah diagram alir dari proses tersebut.



Gambar 3. Proses Analisis dengan CBA

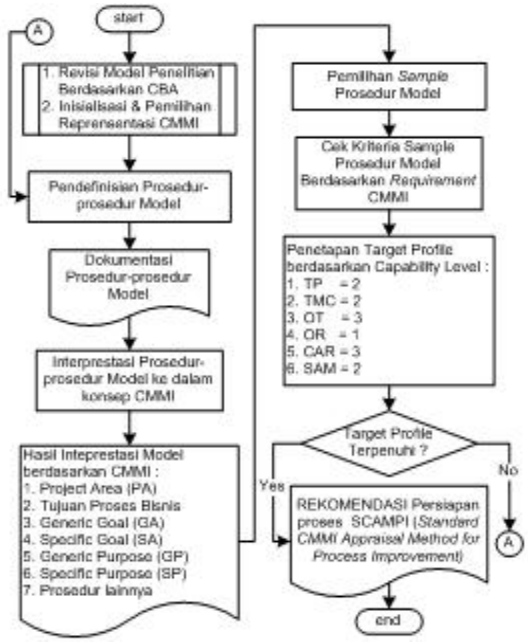
c. *Capability Maturity Model Integration* (CMMI)

CMMI dapat didefinisikan sebagai *suatu pendekatan peningkatan proses yang mendukung organisasi dalam menyediakan elemen-elemen utama bagi suatu proses yang efektif*. [1]

Secara umum CMMI bertujuan,

- memberikan panduan bagi peningkatan proses pada suatu proyek, divisi, atau keseluruhan organisasi[1],
- membantu mengintegrasikan fungsi-fungsi tradisional organisasi yang terpisah-terpisah[1],
- membantu menentukan proses-proses peningkatan tujuan dan prioritas organisasi[1],
- membantu menyediakan panduan peningkatan kualitas proses organisasi[1],
- menyediakan refererensi bagi penilaian proses organisasi[1].

Gambar 4 adalah proses analisis yang akan dilakukan dengan metoda CMMI.



Gambar 4. Proses Analisis dengan CMMI

9. HASIL YANG DIHARAPKAN

Dari keseluruhan proses penelitian diharapkan akan dapat menghasilkan beberapa rekomendasi sebagai berikut:

1) Rekomendasi kelayakan model organisasi CSIRTs berdasarkan sisi ekonomi dan manajemen;
2) Rekomendasi pengimplementasian CSIRTs pada perusahaan berskala besar di Indonesia;
3) Alternatif solusi penanganan insiden keamanan komputer.

10. PENGEMBANGAN PENELITIAN

Pada analisis CMMI, dihasilkan beberapa rekomendasi untuk melanjutkan proses lebih lanjut pada penilaian menurut *Standard CMMI Appraisal Method for Process Improvement* (SCAMPI) Class A. Dimana akan didapat sertifikasi dari CMU/SEI untuk peningkatan proses bisnis pada suatu perusahaan. Sebagai informasi, sertifikasi CMMI ini telah diadopsi oleh sekitar 1,377 perusahaan di dunia.

11. PENUTUP

Penelitian ini dapat menjadi suatu referensi dalam manajemen insiden keamaan sistem informasi. Dimana tujuan yang diharapkan adalah resiko dalam menghadapi insiden keamaanan guna menunjang kelangsungan proses bisnis suatu perusahaan.

PUSTAKA

[1] Ahern, M. Dennis, et. al., (2005), *CMMI® SCAMPI Distilled Appraisals for Process Improvement*, Addison Wesley Professional, Indiana.

[2] Alberts, Chris, et al., (2004), *Defining Incident Management Processes for CSIRTS: A Work in Progress*, Carnegie Mellon University/SEI Paper Notes. CMU/SEI-2003-TR-001, http://www.sei.cmu.edu/publication, 8 Oktober

[3] Arvidsson, Jimmy, (2004), *Taxonomy of the Computer Security Incident related terminology*, TERENA-TF, http://www. ti.terena.nl/teams/, 9 Oktober 2006.

[4] Gordon, A., Lawrence et. al., (2006), *CSI/FBI Computer Crime and Security Survey 2006*, CSI Publication, Washington DC, http://www.GoCSI.com/, 1 November 2006.

[5] Killcrece,Georgia, et. al., (2003), *Organizational Models for Computer Security Response Teams*, Carnegie Mellon University/SEI Paper Notes.CMU/SEI-2003-HB-001, http://www.sei.cmu.edu/publication, 8 Oktober 2006.

[6] Killcrece, Georgia, et. al., (2003), *State of Practice Computer Security Response Teams*, Carnegie Mellon University/SEI Paper Notes.CMU/SEI-2003-TR-001, http://www. sei.cmu.edu/publication, 8 Oktober 2006.

[7] Kumar, Ajoy.,(2005), *CIRT – Framework and Models*, securitydocs.com http://www.securitydocs.com/library/2964, 1 November 2006

[8] Tiktik S. Partomo et. al., (2004), *Ekonomi Skala Kecil/Menengah dan Koperasi*, Ghalia Indonesia, Bogor.

[9] West-Brown, J., Moira, et. al., (2003), *Handbook for Computer Security Response Teams*, Carnegie Mellon University/SEI Paper Notes.CMU/SEI-2003-HB-002, http://www.sei.cmu.edu/publication, 8 Oktober 2003.

[10] Xie. (Nick) Ning, et al., (2004), *SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Project in Small Company*, Carnegie Mellon University/SEI Paper Notes.CMU/SEI-2004-TN-045, http://www.sei.cmu.edu/publication, 22 Oktober 2006.

[11] _____(2006), *Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. 27 Tahun 2006, tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet*, http://www.depkominfo.go.id/, 9 Desember2006.

[12] _____(2006), *Lesson Learn from APEC framework Implementation: Indonesia*, APEC Symposium Information Privacy Protection, http://www.depkominfo.go.id/, Hanoi, 9 Desember2006.