KEBIJAKAN KEAMANAN DENGAN STANDAR BS 7799/ ISO 17799 PADA SISTEM MANAJEMEN KEAMANAN INFORMASI ORGANISASI

Henricus Bambang Triantono
Program Study Computer Accountancy, Faculty Science of Computer, University Bina Nusantara, Jakarta
Jln. KH. Syahdan No. 9 Kemanggisan/Palmerah, Jakarta 11480
e-mail: henricus@binus.ac.id

ABSTRAKSI

Paper ini membahas bagaimana Kebijakan Keamanan dengan standar berdasar pada BS 7799/ISO 17799 pada Sistem Manajemen Keamanan Informasi organisasi digunakan – yaitu memastikan bahwa semua daya upaya terkoordinasi untuk mencapai keamanan yang maksimal. Isu keamanan pada awalnya timbul ketika para ahli komputer ingin bertukar informasi dan menyebarkan ilmu yang dimilikinya. Mereka kemudian menghubungkan sistem komputer secara global dan membiarkan setiap orang bebas untuk mengaksesnya (open concept). Begitu pentingnya aspek keamanan dalam teknologi informasi sehingga beberapa perusahaan pengembang software lantas menjadikan keamanan sebagai prioritas bisnisnya. Software yang "aman" menjadi nilai jual tersendiri bagi perusahaan pengembang dan menjadi pertimbangan utama bagi perusahaan pengguna yang mengutamakan stabilitas sistem dan kerahasiaan datanya. Orang mulai berpikir untuk memproteksi komputer dan tidak membiarkan semua orang bisa mengakses. Sistem Keamanan merupakan salah satu bagian penting dalam setiap proses pengembangan suatu bisnis dan investasi, karena dengan sistem keamanan yang baik resiko atas kehilangan sejumlah nilai yang diinvestasikan menjadi lebih kecil. Keamanan informasi oleh banyak perusahaan masih dianggap sebagai masalah teknis yang cukup ditangani oleh bagian teknologi informasi (TI) saja, sehingga menghasilkan solusi teknologi tanpa melibatkan proses bisnis. Artinya, perangkat lunak dengan sistem keamanan tercanggih pun sering kali belum mencukupi. Kebutuhan atau kemampuan menerapkan semua cara pengamanan sistem, apabila diterapkan dalam sistem dengan teknologi pengamanan mutakhir dan biaya sangat mahal ternyata tidak serumit itu dan fungsinya pun tidak optimum. Tidak ada gunanya membeli sistem murah namun tidak dapat memberikan tingkat keamanan sistem yang diharapkan. Solusi yang ditawarkan kepada perusahaan adalah suatu pedoman atau acuan yang dapat digunakan untuk mengamankan data yang dimilikinya yaitu Standard ISO 17799. Standard ISO 17799 adalah merupakan suatu Standard Informasi Secuity Management System (Sistem Manajemen Keamanan Informasi) yang telah telah disempurnakan untuk digunakan oleh perusahaan didalam mengamankan data yang dimilikinya.

***Kata kunci**: Aspek Keamanan, Teknologi Informasi, Standard ISO 17799*

1. PENDAHULUAN

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai '*quality or state of being secure-to be free from danger*'. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi masing-masing memiliki fokus dan dibangun pada masing-masing kekhususannya. Contoh dari tinjauan keamanan informasi adalah:

- *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal Security* yang overlap dengan '*phisycal security'* dalam melindungi orang-orang dalam organisasi
- *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
- *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Komponen-komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha. Tahun 1990-an dunia TI mulai menyadari kelemahan konsep terbuka tersebut ketika *malware*, istilah teknologi untuk software jahat (*malicious software*), muncul dalam bentuk virus. Seketika itu juga, konsep terbuka berubah menjadi titik lemah sistem

yang memungkinkan virus masuk dan menyerang. Orang pun mulai berpikir untuk memproteksi komputer dan tidak lagi membiarkan semua orang bisa mengakses. Hanya orang kepercayaan dan yang memiliki otorisasi saja yang bisa mengaksesnya, dan kemudian menjadi isu global dalam industri TI. Para ahli software mengamati semua perubahan yang terjadi dan kini telah mendesain program baru untuk mengatasi masalah yang ada. Misalnya, sistem operasi komputer kini telah mengubah standar setting-nya dari bebas akses bagi siapa pun menjadi terbatas dan hanya bisa diakses oleh mereka yang diberi otorisasi. Selanjutnya, setiap software versi baru wajib melewati uji coba dan pengajian ulang serta audit sistem keamanan yang sangat ketat sebelum didistribusikan. Ini sangat penting karena para programer malware akan melancarkan "serangan"-nya begitu mengetahui ada perusahaan pengembang software yang menciptakan program baru. Perangkat lunak dengan sistem keamanan tercanggih pun sering kali belum mencukupi. Agar sistem informasi serta data yang dimiliki dapat lebih terjaga keamanannya, setiap perusahaan atau pengguna komputer harus memerhatikan tiga aspek penting, yaitu teknologi, manusia, dan proses, atau dikenal sebagai segitiga pengaman atau *The Security Triangle*. Aspek pertama, teknologi, telah dibahas panjang lebar di bagaian pendahuluan. Aspek kedua, manusia, yang tidak kalah pentingnya dalam pemastian keamanan sistem teknologi informasi.Aspek manusia ini merupakan paling berharga yang dimiliki suatu perusahaan. Ada tiga hal utama yang perlu diperhatikan dalam aspek manusia.

Pertama, suatu perusahaan hendaknya memiliki staf khusus pengamanan sistem TI. Kebanyakan perusahaan memiliki teknisi TI yang diharapkan bisa melakukan segala sesuatu yang berkenaan dengan TI. Padahal, ahli dalam bidang pengembangan software, misalnya, belum tentu paham tentang hardware dan jaringan komputer. Selain itu, sistem TI bisa jadi sangat rumit sehingga tidak mungkin satu orang mengelola semua aspek yang terkait dengan sistem tersebut. Apabila keamanan merupakan hal yang kritikal bagi perusahaan, seyogianya perusahaan memiliki staf yang terlatih dan ditugaskan khusus untuk mengawasi dan mengamankan sistem tersebut.

Kedua, tidak cukup buat sebuah perusahaan untuk mempekerjakan staf khusus sistem keamanan. Staf tersebut harus dibekali dengan pelatihan secara berkala dan berkelanjutan mengenai standar, teknologi, dan proses karena cepatnya perkembangan dalam dunia teknologi informasi. Pengetahuan dan keterampilan yang dimiliki dua-tiga bulan lalu bisa saja tidak sahih lagi sekarang.

Ketiga, dibutuhkan komitmen dari semua karyawan dalam perusahaan untuk menjaga sistem keamanan TI, seperti komitmen untuk mematuhi aturan mengenai mengenai penggunaan password dan adanya prosedur yang jelas dalam mengakses data. Contoh adalah ketika staf membuka attachment e-mail dari orang tidak dikenal dan ternyata bervirus.

Proses merupakan komponen ketiga dari *The Security Triangle*. Pihak manajemen perusahaan sebaiknya memberikan perhatian cukup tinggi terhadap aspek keamanan proses bisnis serta keamanan data perusahaan. Proses ini antara lain mencakup identifikasi dan analisis risiko bisnis yang terkait dengan sistem TI, pemantauan sistem secara kontinu, dan evaluasi sistem secara berkala guna memastikan keamanan sistem. Apabila dengan diterapkannya sistem TI dengan teknologi pengamanan mutakhir dan biaya sangat mahal kalau ternyata kebutuhannya tidak serumit itu dan fungsinya pun tidak optimum. Sebaliknya, tidak ada gunanya membeli sistem murah namun tidak dapat memberikan tingkat keamanan sistem yang diharapkan. Perusahaan seyogianya mempertimbangkan bobot kebutuhan, manfaat serta biaya yang harus dikeluarkan untuk menjaga keamanan sistemnya. Perusahaan perlu menaksir aset serta kebutuhan bisnisnya, mengidentifikasi dan memprioritaskan risiko yang akan dihadapi dan memperkirakan nilai investasi yang harus dan mampu ditanamkan. Berdasarkan analisis tersebut, perusahaan kemudian membuat dan menerapkan sebuah *action plan*. Setelah itu, perusahaan sebaiknya tetap secara berkala melakukan audit untuk memastikan bahwa sistem tersebut masih cukup andal dan relevan untuk situasi terkini.

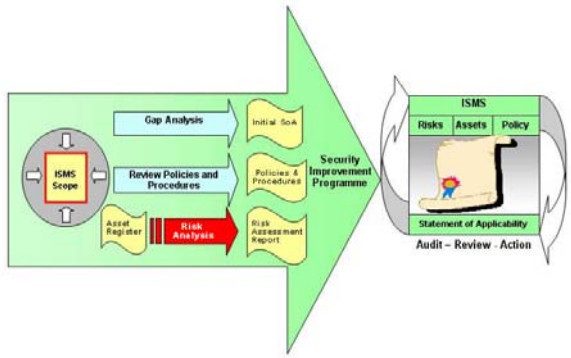
Dari uraian di atas, jelas bahwa keamanan sistem TI bukanlah sederhana. Namun, perusahaan tidak memiliki banyak pilihan selain menerapkannya sesuai dengan kebutuhan. Risiko untuk tidak menerapkan pengamanan TI terlalu besar dan dapat membahayakan jalannnya usaha perusahaan. Tidak satu pun perusahaan sistem komputer atau software yang 100 persen bisa menjamin keamanan sistem. Tidak ada pula perusahaan yang dapat benar-benar merasa aman dari virus, worm atau gangguan lainnya terhadap sistem seberapa pun canggihnya sistem keamanannya. Rasa aman yang semu dapat menyebabkan perusahaan menjadi lengah.

Hal ini semakin menekankan pentingnya setiap perusahaan untuk tetap waspada dan senantiasa memperhatikan ketiga aspek keamanan sistem TI: teknologi, manusia, proses. Dengan demikian, perusahaan dapat meminimalisasi risiko penetrasi virus, worm, ataupun gangguan keamanan sistem TI demi kelangsungan usahanya.

2. THEORITICAL FRAMEWORK

Apa itu suatu *Information Security Managemenr System* –ISMS, System Manajemen Keamanan Informasi menyediakan pendekatan sistematik dalam mengatur informasi yang sensitive agar dapat memproteksinya. ISMS Ini meliputi pegawai, proses-proses dan system informasi itu

sendiri. Keamanan informasi tidak hanya sekedar memasang tembok atau menandatangani kontrak dengan perusahaan keamanan. Dalam bidang ini perlu untuk menggabungkan berbagai inisiatif mengenai strategi perusahaan agar setiap elemen dapat memberikan proteksi yang maksimal. Di sinilah system manajemen keamanan informasi digunakan yaitu memastikan bahwa semua daya upaya terkoordinasi untuk mencapai keamanan yang maksimal. Adapun ruang lingkup dalam ISMS terlihat dalam gambar 1.



Gambar 1. Ruang Lingkup dalam ISMS
Sumber: http://www.boldonjames.com/services/bs7799model.htm

Karena itu system manajemen harus mengikut sertakan metode evaluasi, perlindungan dan proses dokumentasi dan revisi. Ini merupakan prinsip penting dari Perencanaan- Mengerjakan- Pemeriksaan- Pelaksanaan yang sering disebut sebagai Model PDCA yang menggambarkan kualitas manajemen model ISO 9001

2.1 PDCA Model

Gambar 2. PDCA Model
Sumber: The Boldon James PDCA Model

Plan- Perencanaan
Mendefinisikan ruang lingkup ISMS dan kebijakan keamanan organisasi, mengidentifikasi dan menaksir resiko serta menyeleksi tujuan pengawasan, pengawasan membantu untuk mengatur resiko- resiko, dan mempersiapkan pernyataan- pernyataan tentang kegunanaan.

Do- Mengerjakan
Memformulasikan dan mengimplementasikan rencana memperingan resiko, sebelumnya agar mencapai tujuan pengawasan.

Check- Pemeriksaan
Melaksanakan prosedur pelaporan, mengadakan pemeriksaan secara berkala untuk memverifikasi keberhasilan ISMS.

Act- Pelaksanaan
Menjalankan peningkatan ISMS yang terindentifikasi, mengambil tindakan pengkoreksian dan pencegahan yang semestinya, serta memelihara tingkat komunikasi dengan semua pemegang saham

2.2 Kebijakan Keamanan Informasi dengan Standar ISO 17799

Informasi adalah asset penting yang bernilai bagi organisasi dan sangat berharga bagi kelangsungan hidup bisnis serta disajikan dalam berbagai format berupa: catatan, lisan, elektronik, pos, dan audio visual. Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Oleh karena itu, manajemen informasi penting bagi meningkatkan kesuksesan yang kompetitif dalam semua sektor ekonomi. Tujuan manajemen informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi. Dengan tumbuhnya berbagai penipuan, spionase, virus, dan hackers sudah mengancam informasi bisnis manajemen oleh karena meningkatnya keterbukaan informasi dan lebih sedikit kendali/control yang dilakukan melalui teknologi informasi modern. Sebagai konsekwensinya, meningkatkan harapan dari para manajer bisnis, mitra usaha, auditor, dan stakeholders lainnya menuntut adanya manajemen informasi yang efektif untuk memastikan informasi yang menjamin kesinambungan bisnis dan meminimise kerusakan bisnis dengan pencegahan dan memimise dampak peristiwa keamanan. Keamanan informasi terdiri dari perlindungan terhadap elemen-elemen berikut ini:

a) Kerahasiaan: memastikan bahwa informasi dapat di akses hanya oleh pemakai yng berwenang.
b) Integritas: mengamankan keakuratan dan kelengkapan informasi dan cara memproses informasi tersebut.
c) Ketersediaannya: memastikan bahwa pemakai yang berwenang mempunyai akses terhadap informasi dan asset yang berhubungan bilamana diperlukan.

2.3 Standar BS7799/ISO 17799

Pada tahun 1995, Institut Standard Britania (BSI) meluncurkan standard pertama mengenai manajemen informasi terhadap penciptaan struktur

keamanan informasi maka pada awal tahun 1990 BS 7799 di ciptakan, yaitu: "BS 7799, Bagian Pertama: Kode Praktek untuk Manajemen Keamanan Informasi". yang didasarkan pada Infrastruktur pokok BS 7799, ISO (Organisasi Intemasional Standardisasi) yang memperkenalkan ISO 17799 standard mengenai manajemen informasi pada 1 Desember, 2000. Sedangkan bagi ke sepuluh bagian kontrol dari BS 7799/ ISO 17799 standard meliputi: kebijakan keamanan, organisasi keamanan, penggolongan asset dan kendali, keamanan personil, phisik dan kendali lingkungan, pengembangan dan jaringan komputer dan manajemen, sistem akses kendali, pemeliharaan sistem, perencanaan kesinambungan bisnis, dan pemenuhan.

Dalam rangka pro aktif terhadap kebutuhan keamanan, arsitektur keamanan meliputi tiga unsur pokok:

- kebijakan perusahaan (keterlibatan manajemen menyiratkan alokasi sumber daya dan suatu visi yang strategis dan permasalahan global dalam keamanan),
- instrumen teknologi,
- perilaku individu (pelatihan karyawan,dan menciptakan saluran komunikasi).

2.4 Keuntungan dari BS 7799/ISO 17799

Perusahaan yang melakukan penyesuaian dan mengikuti BS 7799/ ISO 17799 bukanlah berarti akan terbebas terjamin keamanannya 100%. Realitasnya, tidak ada satupun di organisasi yang akan mendapatkan keamanan mutlak. Namun demikian setiap manajer harus mempertimbangkan pemakaian standar internasional yang dapat memberikan keuntungan tertentu.

3. PEMBAHASAN

Dalam menciptakan keamanan informasi berikut ini ada sepuluh langkah yang akan dilakukan bila perusahaan betul-betul ingin mewujudkan keamanan informasinya: *Pertama*, mendefinisikan kebijakan keamanan informasi perusahaan. Pengelolaan keamanan informasi yang baik dimulai dengan penyusunan kebijakan keamanan secara tertulis yang menggariskan seluruh persyaratan keamanan untuk dapat memenuhi kepatuhan, standar dan tujuan yang akan dijalankan perusahaan.

Kedua, dapat dilakukan penunjukan penanggung jawab keamanan, dimana penting untuk menunjuk seseorang di dalam perusahaan yang bertanggung jawab kepada tim manajamen untuk menegakkan dan mengamankan informasi di seluruh bagian organisasi.

Ketiga, melakukan inventarisasi aset informasi. Perusahaan harus menyusun daftar aset informasi yang dimilikinya, termasuk peranti lunak, perlengkapan komputer, database, dan file-file, dan mendokumentasikan lokasinya, klasifikasi keamanannya dan pemilik internalnya.

Keempat, melakukan seleksi terhadap staf kunci. Melindungai diri dari ancaman keamanan internal sama pentingnya dengan melindungi diri dari ancaman eksternal.

Kelima, melindungi aset informasi secara fisik. Hal ini memberikan tingkat keamanan informasi yang lebih tinggi. *Keenam*, mempraktikkan pengelolaan jaringan yang efektif. Banyak perusahaan tidak pernah mendokumentasikan prosedur yang benar untuk mengoperasikan sistem-sistem komputer mereka. Hal ini dapat mengakibatkan kegagalan sistem, kehilangan data atau terjadi kebocoran informasi yang sangat berharga dan rahasia.

Ketujuh, menciptakan aturan pengendalian akses yang ketat. Perusahaan harus secara ketat mendefinisikan ijin akses yang diberikan kepada pekerjanya. Hal ini tidak saja dapat menghindari akses tak berwenang ke data rahasia, tetapi juga melindungi integritas sumber komputasi dan melindungi diri dari penggunaan peranti lunak dan yang tidak memiliki kewenangan.

Kedelapan, bangun keamanan di dalam semua sistem dan aplikasi. Jika sebuah perangkat keras atau peranti lunak diinstal, pastikan kompatibilitasnya dengan sistem yang dimiliki untuk menghindari kegagalan sistem, dan mengkonfigurasikan tingkat keamanan yang sesuai sehingga tidak menimbulkan celah kelemahan.

Kesembilan, merencanakan pengembangan terhadap kelangsungan bisnis atau sebuah *contingency plan* yang menggariskan langkah-langkah yang harus diambil perusahaan untuk meminimalkan gangguan jika terjadi bencana dan memulihkan aplikasi penting secepat mungkin agar dapat terus berbisnis.

Kesepuluh, pastikan kepatuhan terhadap peraturan dan UU yang dapat diterapkan. Pendokumentasian dan pengendalian harus diterapkan tidak saja sesuai dengan undang-undang setempat, propinsi atau nasional yang mengatur tata usaha perusahaan.

Sebagai bagian akhir dari bahasan ini dapat disampaikan bahwa lebih dari 80.000 perusahaan di seluruh dunia telah mengikuti BS 7799/ISO 17799, di antaranya adalah Perusahaan Fujitsu, KPMG, Sistem Keamanan Marconi, Perusahaan Electronic Sony, Perusahaan Toshiba. Beberapa faktor- faktor untuk memastikan keberhasilan pengimplementasian manajemen keamanan informasi dalam suatu organisasi yaitu:

1. Kebijakan keamanan, tujuan dan aktivitas keamanan mencerminkan tujuan perusahaan.
2. Melaksanakan pendekatan konsisten terhadap manajemen keamanan perusahaan.
3. Menampakkan dukungan dan komitmen dari manajemen.
4. Suatu pengertian yang baik terhadap syarat-syarat keamanan, penaksiran resiko dan manajemen resiko.
5. Komunikasi yang efektif terhadap persoalan keamanan kepada para manajer dan karyawan.
6. Pendistribusian garis pedoman mengenai kebijakan dan standar keamanan informasi kepada semua karyawan dan leveransir.
7. Pelatihan dan pengajaran yang memadai.

8. Sebuah system pengukuran yang luas dan seimbang yang digunakan untuk mengevaluasi keberhasilan manajemen keamanan informasi dan memberikan saran dan masukan untuk perbaikan.

4. SIMPULAN

a. Keamanan yang baik bukan saja merupakan kemewahan untuk perusahaan-perusahaan besar saja, tetapi juga merupakan keharusan bagi perusahaan kecil. Keamanan informasi disesuaikan dengan perusahaan. Kerahasiaan, integritas, dan keberadaan informasi adalah factor penting dalam memelihara aspek persaingan, arus kas, penyesuaian legalitas dan citra diri perusahaan yang baik.
b. Mengembangkan kebijakan keamanan informasi berdasarkan ISO 17799 merupakan titik utama dalam manajemen keamanan informasi.
c. Salah satu cara terbaik dalam melaksanakan system keamanan informasi yang lengkap dan efektif adalah dengan mengimplementasikan software dan menggunakannya bersama dengan para professional untuk pelayanan intern.
d. Membangun dan menjaga keamanan sistem manajemen informasi akan lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

5. SARAN

a. Keamanan informasi tidak saja merupakan permasalahan teknis-tetapi juga sesuatu yang logis dari sudut pandang bisnis. Oleh karenanya, melindungi asset berupa informasi harus menjadi bagian dari strategi bisnis.
b. Keamanan juga merupakan pekerjaan yang berkesinambungan. Organisasi harus terus meng-update dokumentasi dan sistem sesuai dengan perubahan bisnis.
c. Pastikan berhubungan dengan perusahaan yang etis, serta memiliki reputasi baik dan pengetahuan luas untuk dapat mengkhususkan diri pada solusi serta pada layanan keamanan.

PUSTAKA

Bramanto, Dino B, Country Manager Financial Services Sector PT IBM Indonesia, *Bisnis Indonesia* 5 April 2006.

PERA, Neville Clarke, *Standar Sistem Manajemen Keamanan Informasi* *(bahasa Indonesia) ISO 17799 April 27, 2006

Rizaldy, Arif, Technology Specialist Microsoft Indonesia" Penerapan Segitiga Pengaman Aspek Penting Melindungi Sistem Teknologi" *KOMPAS*, 16 Agustus 2004

www.callio.com Callio Technologies BS7799/ ISO17799 solution ""Mengimplementasi Kebijakan Keamanan dengan Standar BS 7799/ISO 17799.

www.boldonjames.com/services/bs7799model.htm

www.boldonjames.com/services/pdcamodel.htm
The Boldon James PDCA Model