INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) MENGGUNAKAN STANDAR ISO/IEC 27001:2005

Melwin Syafrizal
Dosen STMIK AMIKOM Yogyakarta

Abstraksi

Informasi adalah salah satu asset penting yang sangat berharga bagi kelangsungan hidup suatu organisasi atau bisnis, pertahanan keamanan dan keutuhan negara, kepercayaan publik atau konsumen, sehingga harus dijaga ketersediaan, ketepatan dan keutuhan informasinya. Informasi dapat disajikan dalam berbagai format seperti: teks, gambar, audio, maupun video. Tersimpan dalam komputer atau media penyimpanan external lain (seperti: harddisk, flashdisk, CD, DVD, dan lain-lain), tercetak / tertulis dalam media kertas atau media bentuk lainnya.

Manajemen pengelolaan informasi menjadi penting ketika terkait dengan kredibilitas dan kelangsungan hidup orang banyak. Perusahaan penyedia jasa teknologi informasi (TI), media pemberitaan, transportasi, perbankan hingga industri lainnya yang sedikit sekali bersentuhan dengan teknologi informasi, seperti: perusahaan penyedia makanan, penginapan, pertanian, peternakan dan lain-lain. Ketika perusahaan menempatkan informasi sebagai infrastruktur kritikal (penting), maka pengelolaan keamanan informasi yang dimiliki menjadi prioritas utama demi kelangsungan hidup dan perkembangan perusahaan.

Kata Kunci: Information Security, ISMS, ISO

Pendahuluan

Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau ter-ekspos-nya data ke pihak eksternal yang tidak diinginkan.

Bersikap ”over protektif” terhadap informasi yang dimiliki, mungkin dapat membuat kita lelah dengan terus menerus mengawasinya, merasa was-was bila sebentar saja meninggalkannya. Para pekerja, mitra usaha juga pelanggan, menjadi tidak nyaman karena merasa tidak dipercaya. Membuka secara luas akses terhadap informasi penting dan rahasia, mungkin bukan hal yang bijaksana. Faktor-faktor tersebut dapat membuat pemilik informasi bingung harus bersikap bagaimana.

Sistem pengelolaan keamanan informasi dalam hal ini, menjadi penting untuk dipahami, diupayakan atau dicoba untuk diimplementasikan agar informasi dapat dikelola dengan benar, sehingga perusahaan atau instansi dapat lebih fokus mencapai visi yang sudah ditetapkan, atau melakukan hal-hal lain untuk perkembangan usaha, atau lebih fokus dalam memberikan layanan terbaik bagi pelanggan (masyarakat).

Teknologi bukanlah satu-satunya aspek yang harus kita perhatikan ketika mempertimbangkan serta memikirkan bagaimana cara yang paling baik untuk memastikan bahwa data dan informasi perusahaan tidak diakses oleh pihak-pihak yang tidak memiliki hak. **Proses dan manusia** adalah dua aspek yang tidak kalah pentingnya.

Pembahasan

Kejadian berikut ini merupakan kejadian nyata yang terjadi di sebuah perusahaan besar di Indonesia. Namun, beberapa aspek dari kejadian ini harus penulis samarkan dengan beberapa alasan. Pada awal tahun

2006, PT “A” geger, dikarenakan pada suatu pagi di hari Senin, ketika semua karyawan mulai kembali beraktivitas setelah libur panjang, sebuah e-mail masuk ke seluruh *mailbox* karyawan dengan sebuah *attachment* berupa file excel yang di dalamnya berisi data dan informasi gaji ribuan karyawan di perusahaan tersebut.

Coba bayangkan efek dari kejadian ini, ketika tiba-tiba seorang karyawan menjadi tahu gaji rekannya yang kebetulan memiliki tingkat pekerjaan yang sama, namun bergaji jauh lebih tinggi. Begitu pula seorang staf yang tiba-tiba mengetahui gaji atasannya.

Investigasi dengan serta-merta pun dilakukan oleh pihak teknologi informasi perusahaan tersebut dengan dipimpin langsung oleh vice president IT. Karena file excel tersebut dikirim melalui e-mail, maka pasti ada pengirimnya, sebut saja Bapak ‘B’. Namun penyelidikan kemudian menemukan jalan buntu, karena pada hari serta tanggal pengiriman yang tertera pada e-mail, Bapak ‘B’ ini sedang bertugas di salah satu lokasi kantor cabang yang tidak memiliki koneksi Internet, dan ada banyak saksi yang bersedia memberikan keterangan bahwa beliau sama sekali tidak dapat mengakses sistem e-mail perusahaan selama sehari penuh bahkan hingga beberapa ke depan.

Investigasi secara teknis pun dilakukan dengan memeriksa *access log,* baik pada sistem e-mail maupun LDAP untuk melihat siapa saja staf atau karyawan di perusahaan tersebut yang melakukan akses pada hari dan jam terkirimnya e-mail tersebut. Namun celakanya, seseorang dengan cerdiknya telah berhasil menghapus “jejak”, sehingga tim penyelidik kembali mendapatkan hasil nol besar. Kesimpulan sementara dari hasil penyelidikan akhirnya hanya mengindikasikan bahwa Bapak “B” telah dijebak, dan seseorang dengan tingkat pengetahuan serta *skill* teknis yang cukup tinggi, telah mengakses data dan informasi gaji tersebut dari pihak *payroll*, mengirimnya dengan menggunakan e-mail account Bapak ‘B’, lalu dengan cerdik menghapus semua jejaknya. Tanpa tahu siapa yang sebenarnya telah melakukan tindakan ini serta apa motifnya.

Tim investigasi internal juga melakukan beberapa perubahan konfigurasi pada sistem e-mail perusahaan serta memperketat aktivitas pengawasan secara digital yang antara lain adalah memusatkan penyimpanan log-log aktivitas setiap system di dalam *data center*. Hal ini diharapkan akan dapat menghindari kejadian-kejadian yang sama di masa depan. Selesai sampai di sini? Ternyata tidak. Tepat satu bulan kemudian, e-mail heboh tersebut kembali terkirim ke seluruh mailbox karyawan PT "A", masih dengan isi yang sama dan pengirim yang sama, dan kembali terulang lagi untuk ketiga kalinya di bulan berikutnya.

Kejadian tersebut juga memberikan gambaran kepada kita bahwa sekuat apapun kita memasang perangkat keamanan di infrastruktur teknologi informasi di kantor, katakanlah sistem *firewall* tiga lapis dengan merek yang berbeda-beda, antivirus yang juga diimplementasikan secara komplementer dari dua merk berbeda serta keamanan fisik lainnya seperti implementasi perangkat biometric di data center. Masih belum cukup untuk "mengusir" tangan-tangan jahil orang-orang yang tidak bertanggung jawab.

PT "A" seperti contoh di atas, bukanlah sebuah perusahaan yang "pemula" di bidang teknologi informasi. Investasi teknologi informasi perusahaan ini pernah pada suatu tahun fiskal tertentu nyaris mendekati angka Rp 1 milyar. Pembangunan sistem serta teknologi informasinya juga dipandu langsung oleh sebuah perusahaan integrasi sistem terbesar di dunia. Namun ternyata semua itu masih belum cukup, karena sebuah data yang sifatnya rahasia ternyata masih juga dapat tersebar hingga menyebabkan terjadinya perubahan suasana kerja yang cukup signifikan terhadap produktivitas perusahaan.

Dampak psikologis, baik secara organisasi maupun perorangan dari kejadian ini ternyata cukup masif kuantitas dan kualitasnya. Akhirnya beberapa perubahan serta tindakan pencegahan yang cukup agresif dilakukan oleh pihak manajemen dengan tujuan agar kejadian tersebut tidak lagi terulang di masa depan.

Information Security Management System (ISMS) merupakan sebuah kesatuan sistem yang disusun berdasarkan pendekatan resiko bisnis untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan.

Sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut yang menjadi objek yang akan diteliti, antara lain:

- **Struktur organisasi**
- **Kebijakan keamanan (security policy)**
- **Prosedur dan proses**
- **Tanggung jawab atau responsibility**
- **Sumber Daya Manusia**

Masalah yang ingin diteliti pada objek penelitian ini, adalah

- **Struktur organisasi pengelola jaringan dan keamanan informasi**. ”apakah struktur organisasi yang ada saat ini sudah mengakomodir kebutuhan akan orang atau departemen yang bertanggung jawab secara khusus untuk membangun jaringan komputer dan sistem informasi yang secara terus menerus dimonitoring, dikembangkan, dijaga keamanan dan ketersediaannya?
- **Tindakan preventif dan kepedulian pengguna jaringan yang memanfaatkan informasi.** Apakah semua permasalahan jaringan dan kejadian pelanggaran keamanan atas setiap kelemahan sistem informasi telah ”segera” dilaporkan sehingga administrator (jaringan maupun database perusahaan) akan segera mengambil langkah-langkah keamanan yang dianggap perlu.
- Apakah **akses terhadap sumber daya pada jaringan** sudah dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak.

- Apakah **akses terhadap sistem komputasi dan informasi serta periferalnya** juga koneksi ke jaringan telah diatur dengan baik, termasuk logon pengguna.
- Apakah **pengelolaan account** sudah dikelola secara benar untuk menjamin bahwa hanya orang/peralatan yang diotorisasi yang dapat terkoneksi ke jaringan?
- **A**pakah semua **prosedur serta proses-proses yang terkait dengan usaha-usaha pengimplementasian keamanan informasi** di perusahaan sudah dijalankan dengan benar?" Misalnya prosedur permohonan ijin akses aplikasi, akses *hotspot*, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.
- Sudahkah perusahaan melaksanakan ketentuan dimaksud dan memberikan **pelatihan dan sosialisasi** yang cukup bagi **setiap individu** untuk **sadar akan pentingnya upaya menjaga keamanan informasi**?
- **Policy dan tindakan yang ditetapkan** perusahaan dalam melindungi sistem keamanan jaringan dan informasi apakah sudah dilaksanakan dengan benar?.

Tujuan Implementasi ISO 27001

Implementasi ISO/IEC 27001:2005 ini bertujuan untuk memberikan gambaran implementasi sistem manajemen keamanan informasi berstandar internasional kepada perusahaan, organisasi nirlaba, instansi atau publik agar dapat mempelajari dan mencoba mengimplementasikannya dilingkungan sendiri.

Implementasi ISO/IEC 27001:2005 pada kegiatannya juga mencoba melakukan kegiatan audit terhadap semua aspek terkait, seperti: kondisi jaringan komputer lokal, policy, manajemen SDM, organisasi keamanan informasi, dan lain-lain.

Tujuan Audit dan Manfaat Penetapan ISO/IEC 27001:2005

- Audit ISMS memberi pemahaman yang lebih baik mengenai aset informasi dan proses manajemen keamanan informasi yang diperlukan.
- Membantu memberikan pemahaman pentingnya keamanan informasi pada karyawan, stakeholder dan masyarakat umum,
- Membantu mengarahkan implementasi sistem manajemen keamanan informasi berdasarkan kepada pertimbangan manajemen risiko.
- Mendukung organisasi dengan memberi kerangka kerja (panduan) proses untuk mengimplementasikan dan melakukan manajemen serta kontrol terhadap keamanan informasi agar dapat menjamin bahwa objek-objek keamanan tertentu telah dicapai.
- Membantu organisasi untuk menjaminkan risiko keamanan dapat dikendalikan dengan biaya terkontrol dan dengan feedback yang menguntungkan,
- Meningkatkan keyakinan terhadap organisasi karena telah mematuhi undang-undang, peraturan-peraturan negara, dengan menjamin kualitas informasi dan pelayanan.
- Mempersilakan auditor internal maupun external untuk memastikan bahwa organisasi telah mematuhi aturan-aturan, memiliki arah pengembangan Manajemen dan standard-standard yang dilaksanakan.
- Simbol untuk kualitas dan keamanan. Penetapan ISO/IEC 27001:2005 akan menunjukkan kepada pelanggan-pelanggan, partner anda dan pihak pemerintah bahwa kualitas pelayanan dan keamanan yang baik dalam proses bisnis anda telah dikendalikan dengan benar, hal ini dapat menjadi publikasi yang sangat positif bagi organisasi untuk meraih kepercayaan stake holder.

Tinjauan Pustaka dan Landasan Teori

Keamanan Informasi

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa "keamanan informasi" dan bukan "keamanan teknologi informasi" atau IT Security. Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. "Keamanan Teknologi Informasi" atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

Berbeda dengan "keamanan informasi" yang fokusnya justru pada data dan informasi milik perusahaan Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

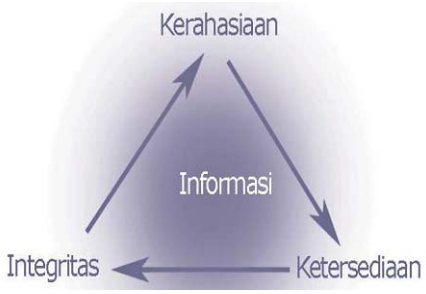
Berdasarkan penjelasan tersebut, 'kemananan teknologi informasi' merupakan bagian dari keseluruhan aspek 'keamanan informasi'. Karena teknologi informasi merupakan salah satu alat atau tool penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, kita akan mengetahui bahwa teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di perusahaan.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

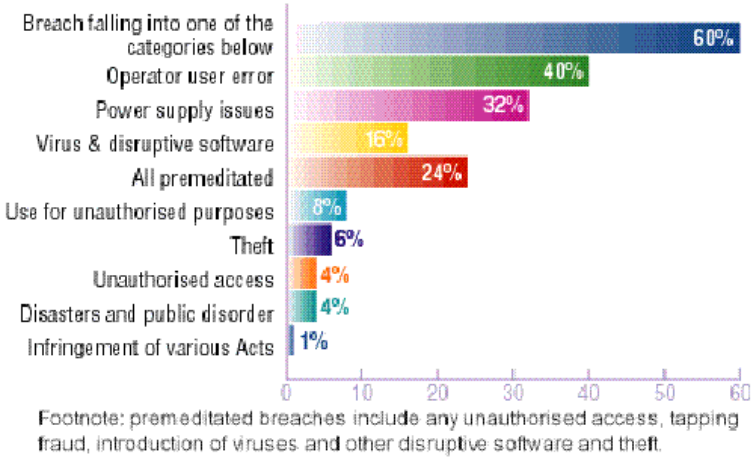


Gambar 1 Elemen-elemen Keamanan Informasi

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.

Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak

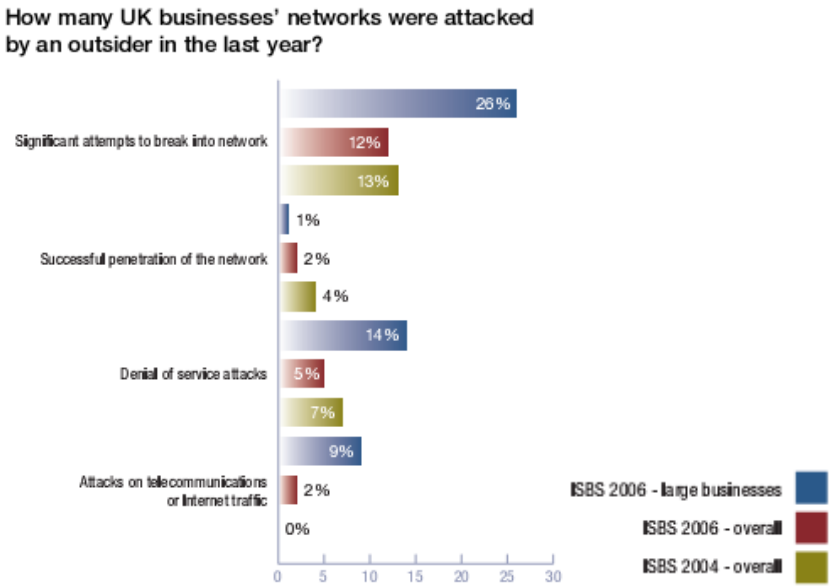
cukup terpelihara/terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:



Gambar 2 Grafik Persentase Ancaman Keamanan Sistem Informasi

Survey tersebut juga menunjukkan bahwa 60% organisasi mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan. Kegagalan sistem keamanan lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Faktor internal ini diantaranya kesalahan dalam pengoperasian sistem (40%) dan diskontinuitas power supply (32%).

Hasil survey ISBS tahun 2004-2006 menunjukkan bahwa terdapat banyak jaringan bisnis di Inggris (UK) telah mendapatkan serangan dari luar.



Gambar 3 UK Business Network Attack

Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

Dasar Manajemen Keamanan Informasi

Informasi Sebagai Aset

Informasi adalah salah satu aset bagi sebuah perusahaan atau organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi perusahaan atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan perusahaan atau organisasi, meminimalisir

kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha [1]. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan atau organisasi meliputi diantaranya: informasi yang tersimpan dalam komputer (baik *desktop* komputer maupun *mobile* komputer), informasi yang ditransmisikan melalui network, informasi yang dicetak pada kertas, dikirim melalui fax, tersimpan dalam disket, CD, DVD, flashdisk, atau media penyimpanan lain, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dikirim melalui telex, email, informasi yang tersimpan dalam database, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi yang lain, dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide baru organisasi atau perusahaan [2].

Informasi perlu dilindungi keamanannya

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai "*quality or state of being secure-to be free from danger"* [1]. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi memiliki fokus dan dibangun pada masing-masing ke-khusus-annya. 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.

Masing-masing komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya [2]. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha [3].

Aspek Lain Keamanan Informasi

Keamanan informasi memiliki beberapa aspek yang harus dipahami untuk dapat diterapkan. Beberapa aspek tersebut, tiga yang pertama disebut C.I.A (*Confidentiality, Integrity & Availability) "triangle model"* [Gambar 3.1 Elemen-elemen keamanan informasi], seperti yang diuraikan pada point 3.1 Keamanan Informasi (pembahasan sebelumnya).

Aspek yang lain disebutkan oleh Dr. Michael E.Whitman dan Herbert J. Mattord dalam bukunya Management Of Information Security adalah:

- *Privacy*

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik.

- *Identification*

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *user name* atau *user ID.*

- *Authentication*

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang mereka klaim.

- *Authorization*

Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.

- *Accountability*

Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktifitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktifitas itu.

Manajemen

Sangat penting memahami beberapa prinsip dalam manajemen. Secara sederhana, manajemen adalah proses untuk mencapai tujuan dengan

menggunakan sumberdaya yang ada [3]. Manajer adalah seseorang yang bekerja dengan orang lain dan melalui orang lain dengan cara mengkoordinasi kerja mereka untuk memenuhi tujuan organisasi. Tugas manajer adalah untuk memimpin pengelolaan sumberdaya organisasi, melakukan koordinasi penyelesaian pekerjaan orang-orang dalam organisasi, dan memegang aturan-aturan yang diperlukan untuk memenuhi tujuan organisasi. Diantara aturan-aturan itu adalah:

- *Aturan informasi*: mengumpulkan, memproses, dan menggunakan informasi yang dapat mempengaruhi pencapaian tujuan.
- *Aturan interpersonal*: berinteraksi dengan *stakeholder* dan orang atau organisasi lain yang mempengaruhi atau dipengaruhi oleh tercapainya tujuan organisasi dimana dia menjadi manajer.
- *Aturan keputusan*: memilih diantara beberapa alternatif pendekatan, memecahkan konflik, dilema atau tantangan.

Manajer mengelola sumberdaya organisasi meliputi perencanaan biaya organisasi, otorisasi pengeluaran biaya, dan menyewa pekerja.

Manajemen Keamanan Informasi

Sebagaimana telah disebutkan sebelumnya bahwa manajemen keamanan informasi adalah satu dari tiga bagian dalam komponen keamanan informasi menurut NSTISSC. Sebagai bagian dari keseluruhan manajemen, tujuan manajemen keamanan informasi berbeda dengan manajemen teknologi informasi dan manajemen umum, karena memfokuskan diri pada keamanan operasi organisasi. Manajemen keamanan informasi memiliki tanggung jawab untuk program khusus, maka ada karakteristik khusus yang harus dimilikinya, yang dalam manajemen keamanan informasi dikenal sebagai 6P yaitu:

Planning

Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

1) *strategic planning* yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,
2) *tactical planning* memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,
3) *operational planning* memfokuskan diri pada kinerja harian organisasi. Sebagi tambahannya, planning dalam manajemen keamanan informasi adalah aktifitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi. Ada beberapa tipe planning dalam manajemen keamanan informasi, meliputi :

   - *Incident Response Planning (IRP)*

     IRP terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam *confidentiality*, *integrity* atau *availbility* sumberdaya informasi. *Insident Response Planning* meliputi *incident detection*, *incident response*, dan *incident recovery*.

   - *Disaster Recovery Planning* (DRP)

Disaster Recovery Planning merupakan persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana. Pada beberapa kasus, insiden yang dideteksi dalam IRP dapat dikategorikan sebagai bencana jika skalanya sangat besar dan IRP tidak dapat lagi menanganinya secara efektif dan efisien untuk melakukan pemulihan dari insiden itu. Insiden dapat kemudian dikategorikan sebagai bencana jika organisasi tidak mampu mengendalikan akibat dari insiden yang terjadi, dan tingkat kerusakan yang ditimbulkan sangat besar sehingga memerlukan waktu yang lama untuk melakukan pemulihan.

❖ *Business Continuity Planning* (BCP)

Business Continuity Planning menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Identifikasi fungsi kritis organisasi dan sumberdaya pendukungnya merupakan tugas utama business continuity planning. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

Policy

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

- *Enterprise Information Security Policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
- *Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.

- *System Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

Programs

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

Protection

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

People

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

Project Management

Komponen terakhir adalah penerapan kedisiplinan manajemen dalam setiap elemen kemanan informasi. Hal ini melibatkan identifikasi dan pengendalian sumberdaya yang dikerahkan untuk

keamanan informasi, misalnya pengukuran pencapaian keamanan informasi dan peningkatannya dalam mencapai tujuan keamanan informasi.

Perlunya Manajemen Keamanan Informasi

Manajemen keamanan informasi diperlukan karena ancaman terhadap C.I.A (*triangle model*) aset informasi semakin lama semakin meningkat. Menurut survey UK Department of Trade and Industry pada tahun 2000, 49% organisasi meyakini bahwa informasi adalah aset yang penting karena kebocoran informasi dapat dimanfaatkan oleh pesaing, dan 49% organisasi meyakini bahwa keamanan informasi sangat penting untuk memperoleh kepercayaan konsumen. Organisasi menghadapi berbagai ancaman terhadap informasi yang dimilikinya, sehingga diperlukan langkah-langkah yang tepat untuk mengamankan aset informasi yang dimiliki.

Standarisasi Sistem Manajemen Keamanan Informasi

Ada banyak sekali model manajemen keamanan informasi dan penerapannya, karena banyaknya konsultan keamanan informasi yang menawarkannya, masing-masing memfokuskan diri pada area yang berbeda dalam praktek manajemen keamanan informasi.

- BS 7799:1, sekarang dikenal sebagai ISO/IEC 17799 setelah diadopsi oleh ISO, disebut sebagai Information Technology Code of Practice for Information Security Management.
- BS 7799:2 disebut sebagai Information Security Management: Specification with Guidance for Use.
- ISO/IEC 27001 adalah standar information security yang diterbitkan pada Oktober 2005 oleh International Organization for Standarization (ISO) dan International

Electrotechnical Commission (IEC). Standar ini menggantikan BS-77992:2002 (British Standard).

- General Accepted System Security Principles atau "GASSP", yang merupakan bagian dari kumpulan penerapan sistem keamanan informasi.
- Guidelines for the Management of IT Security, atau GMITS / ISO-13335, yang menyediakan sebuah konsep kerangka kerja (framework) untuk manajemen keamanan IT.

Mendapatkan dokumen Standar ISO ini, organisasi/perusahaan/istansi yang akan menerapkannya harus membayarnya dan biasanya meminta bimbingan fihak konsultan yang memahami proses sertifikasi ISO tersebut.

ISO/IEC 27001: 2005

ISO/IEC 27001 adalah standar information security yang diterbitkan pada October 2005 oleh International Organization for Standarization dan International Electrotechnical Commission. Standar ini menggantikan BS-77992:2002.

ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara seta mendokumentasikan Information Security Management System dalam konteks resiko bisnis organisasi keseluruhan

ISO/IEC 27001 mendefenisikan keperluan-keperluan untuk sistem manajemen keamanan informasi (ISMS). ISMS yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ISMS ini akan

memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

Information Security Management System

Information Security Management System (ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

- **Struktur organisasi**, biasarnya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; Chief Security Offi cer dan beberapa lainnya.
- **Kebijakan keamanan,** atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.
- **Prosedur dan proses,** yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.
- **Tanggung jawab**, yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek

keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

- **Sumber daya manusia**, adalah pelaksana serta obyek pengembangan keamanan informasi di perusahaan. Manusia yang bisa memperbaiki serta merusak semua usaha-usaha tersebut.

Serial ISO 27000

International Standards Organization (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000. Adapun beberapa standar di seri ISO ini adalah sebagai berikut:

- **ISO 27000:** dokumen defenisi-defenisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
- **ISO 27001**: berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan
- **ISO 27002**: terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.
- **ISO 27003**: panduan implementasi sistem manajemen keamanan informasi perusahaan.
- **ISO 27004**: dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.
- **ISO 27005**: dokumen panduan pelaksanaan manajemen risiko.
- **ISO 27006**: dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.
- **ISO 27007**: dokumen panduan audit sistem manajemen keamanan informasi perusahaan.
- **ISO 27799**: panduan ISO 27001 untuk industri kesehatan.

ISO 27001: 2005 digunakan sebagai icon sertifikasi ISO 27000. ISO 27001: 2005 merupakan dokumen standar sistem

manajemen keamanan informasi atau *Information Security Managemen System*–ISMS yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di perusahaan. Secara umum ada 11 aspek atau yang biasa disebut sebagai *control*, yang harus ada dalam setiap perusahaan dalam usahanya mengimplementasikan konsep keamanan informasi.

Control dalam hal ini adalah hal-hal, bisa berupa proses, prosedur, kebijakan maupun *tool* yang digunakan sebagai alat pencegahan terjadinya sesuatu yang tidak dikehendaki oleh adanya konsep keamanan informasi, seperti akses terlarang terhadap data atau informasi rahasia perusahaan.

Adapun ke-11 control tersebut adalah sebagai berikut:

- Security policy.
- Organization of information security.
- Asset management.
- Human resources security.
- Physical and environmental security.
- Communications and operations management.
- Access control.
- Information system acquisition, development, and maintenance.
- Information security incident management.
- Business continuity management.
- Compliance.

Bagaimana ISO/IEC 27001:2005 Dijalankan

Penilaian risiko dan manajemen yang benar adalah faktor terpenting dalam ISO/IEC 27001. Standar ini membolehkan organisasi

memperkenalkan objek-objek pengawasan dan memilih cara-cara penyelenggaraan keamanan yang paling sesuai. Jika organisasi ingin memulai menerapkan standard ini, maka mulai dengan mendefinisikan semua permasalahan dan faktor-faktor yang terkait secara sistematik dan cara-cara manajemen risiko yang sudah atau akan diterapkan (direncanakan).

Pendefenisian ini bertujuan untuk memberikan pendekatan terhadap pengelolaan (manajemen) risiko yang akan ditetapkan dalam bentuk aturan-aturan, terkait dengan penilaian risiko oleh tim auditor (fihak organisasi sendiri atau konsultan yang memahami standar ini) untuk memastikan peringkat keamanan yang diperlukan sesuai dengan kondisi anggaran keuangan organisasi.

Objek-objek dan cara-cara kontrolnya dapat dilihat pada lampiran ISO/IEC 27001:2005 agar dapat mencapai keperluan-keperluan yang diperkenalkan (hasil maksimal yang diharapkan) dalam penilaian risiko dan proses pemulihannya. Jika sistem keamanan yang telah diwujudkan sudah sampai taraf memuaskan, maka kontrol yang diuraikan dalam lampiran dapat diabaikan. Kontrol dan evaluasi yang ekstra ketat dapat juga diterapkan. Setelah mampu mengimplementasikan manajemen risiko yang tersistematis, organisasi dapat menetapkan bahwa sistemnya telah sesuai untuk keperluan-keperluan sendiri dan standard.

Kendala penerapan ISMS

Meskipun ISO/IEC 27001 sudah memberikan gambaran lengkap mengenai ketatalaksanaan sistem manajemen keamanan informasi, tetapi terdapat kesulitan dalam menerapkannya disebabkan kurangnya perhatian banyak orang terhadap pentingnya sistem manajemen keamanan informasi (terutama Top Manajemen). Kesulitan penerapan ini meliputi pemilihan metode pendekatan untuk risk assessment, melakukan identifikasi resiko, memperkirakan resiko, dan memilih kendali yang tepat untuk diterapkan.

Daftar Pustaka

Ferdinand Aruan (2003), Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 - Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi ITB

Indocommit (23 Desember 2005), Kepatuhan terhadap Sistem Keamanan Informasi http://www.indocommit.com/index.html?menu=29&idnews=1506&kid=0&PHPSESSID=ac0fa9bf4b764ea21e26b230102b4ecb,

Jacquelin Bisson, CISSP (Analis Keamanan Informasi, Callio Technologies) & René Saint-Germain (Direktur Utama, Callio Technologies), Mengimplementasi kebijakan keamanan dengan standar BS7799 /ISO17799 untuk pendekatan terhadap informasi keamanan yang lebih baik, White Paper, http://202.57.1.181/~download/linux_opensource/artikel+tutorial/ general_tutorials/wp_iso_id.pdf

Jimmy Hannytyo Pinontoan (28/12/2007), Manajemen Keamanan Informasi dengan ISO27001 & ISO27002 http://www.pcmedia.co.id/detail.asp? Id=1914&Cid=22&Eid=49

News Release (April 27, 2006), ISO17799: Standar Sistem Manajemen Keamanan Informasi http://www.nevilleclarke.com/newsReleases/newsController.php?do=toNews&id=45

Puguh Kusdianto (2005), Tugas Akhir EC5010 Keamanan Sistem Informasi, judul Konsep Manajemen Keamanan Informasi ISO-17799 dengan Risk Assessment Menggunakan Metode OCTAVE

Sany Asyari (26 September 2006), Keamanan Jaringan Berdasarkan ISO 17799, http://sanyasyari.com/2006/09/26/keamanan-jaringan-berdasarkan-iso17799/