MODUL KULIAH ONLINE 10

FEB 501 – SISTEM INFORMASI MANAJEMEN

KEAMANAN INFORMASI PADA SISTEM INFORMASI MANAJEMEN

A. KEBUTUHAN ORGANISASI AKAN KEAMANAN DAN PENGENDALIAN

Dalam dunia masa kini, banyak organisasi semakin sadar akan pentingnya menjaga seluruh sumber daya mereka, baik yang bersifat virtual maupun fisik agar aman dari ancaman baik dari dalam atau dari luar. Sistem komputer yang pertama hanya memiliki sedikit perlindungan keamanan, namun hal ini berubah pada saat perang viaetnam ketika sejumlah instalasi keamanan komputer dirusak pemrotes. Pengalaman ini menginspirasi kalangan industri untuk meletakkan penjagaan keamanan yang bertujuan untuk menghilangkan atau mengurangi kemungkinan kerusakan atau penghancuran serta menyediakan organisasi dengnan kemampuan untuk melanjutkan kegiatan operasional setelah terjadi gangguan.

Pendekatan-pendekatan yang dimulai di kalangan industri dicontoh dan diperluas. Ketika pencegahan federal ini diimplementasikan, dua isu penting harus diatasi yakni keamana versus hak-hak individu dan keamaan versus ketersediaan.

B. KEAMANAN INFORMASI

Saat pemerintah dan kalangan industri mulai menyadari kebutuhan untuk mengamankan sumber daya informasi mereka, perhatian nyaris terfokus secara eksklusif pada perlindunga peranti keras data maka istilah keamanan sistem digunakan. Istilah keamanan sistem digunakan untuk mengambarkan perlindungna baik peralatan komputer dan nonkomputer, fasilitas,data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang.

Tujuan Keamanan Informasi

Keamanan informasi ditujuakn untuk mencapai tiga tujuan utama yakni:

a. Kerahasiaan. Perusahaan berusaha untuk melindungi data dan informasinya dari pengungkapan orang-orang yang tidak berwenang.

b. Ketersediaan. Tujuan dari infrastruktur informasi perusahaan adalah menyediakan data dan informasi bagi pihak-pihak yang memiliki wewenang untuk menggunakannya.
c. Integritas. Semua sistem informasi harus memberikan representasi akurat atas sistem fisik yang direpresentasikannya.

Manajemen Keamanan informasi

Aktivitas untuk menjaga agar sumber daya informasi tetap aman disebut manajemen keamanan informasi (information security management – ISM), sedangkan aktivitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah adanya bencana disebut manajemen keberlangsungan bisnis (bussiness continuity management – BCM).

Jabatan direktur keamanan sistem informasi perusahaan (coorporate information system security officer – CISSO) digunakan untuk individu di dalam organisasi, biasanya anggota dari unit sistem informasi yang bertanggung jawab atas keamanan sistem informasi perusahaan tersebut.

C. MANAJEMEN KEAMANAN INFORMASI

Pada bentuknya yang paling dasar, manajemen keamanan informasi terdiri atas empat tahap yakni:

a. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
b. Mendefenisikan risiko yang dapat disebabkan oleh ancaman-ancaman tersebut
c. Menentukan kebijakan keamanan informasi
d. Mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut.

Istilah manajemen risiko (risk management) dibuat untuk menggambarkan pendekatan ini dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.

Tolak ukur (benchmark) adalah tingkat kinerja yag disarankan. Tolak ukur keamanan informasi (information security benchmark) adalah tingkat kemanan yang disarankan yang dalam keadaan normal harus menawarkan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi.standar atau tolak ukur semacam ini ditentukan oleh pemerintah dan asosiasi industri serta mencerminkan komponen-komponen program keamanan informais yang baik menurut otoritas tersebut.

Ketika perusahaan mengikuti pendekatan ini, yang disebut kepatuhan terhadap tolak ukur (benchmark compliance) dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolak ukur tersebut menawarkan perlindungan yang baik.

D. ANCAMAN

Ancaman Keamanan Informasi (Information Security Threat) merupakan orang, organisasi, mekanisme, atauperistiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Pada kenyataannya, ancaman dapat bersifat internal serta eksternal dan bersifat disengaja dan tidak disengaja.

Ancaman Internal dan Eksternal

Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut.

Ancaman internal diperkirakan menghasilkan kerusakan yang secara potensi lebih serius jika dibandingkan denga ancaman eksternal, dikarenakan pengetahuan anccaman internal yang lebih mendalam akan sistem tersebut. Ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha.

Tindakan Kecelakaan dan disengaja

Tidak semua ancaman merupakan tindakan disengaja yang dilakukan dengan tujuan mencelakai. Beberapa merupakan kecelakaan yang disebabkan oelh orang-orang di dalam ataupun diluar perusahaan. sama halnya

Jenis- Jenis Ancaman:

Malicious software, atau malware terdiri atas program-program lengkap atau segmen-segmen kode yang dapat menyerang suatu system dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemilik system. Fungsi-fungsi tersebut dapat menghapus file,atau menyebabkan sistem tersebut berhenti. Terdapat beberapa jensi peranti lunak yang berbahaya, yakni:

a. Virus. Adalah program komputer yang dapat mereplikasi dirinya sendiri tanpa dapat diamati oleh si pengguna dan menempelkan salinan dirinya pada program-program dan boot sector lain
b. Worm. Program yang tidak dapat mereplikasikan dirinya sendiri di dalam sistem, tetapi dapat menyebarkan salinannya melalui e-mail
c. Trojan Horse. Program yang tidak dapat mereplikasi atau mendistribusikan dirinya sendiri, namun disebarkan sebagai perangkat
d. Adware. Program yang memunculkan pesan-pesan iklan yang mengganggu
e. Spyware. Program yang mengumpulkan data dari mesin pengguna

E. RISIKO

Risiko Keamanan Informasi (Information Security Risk) didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Risiko-risiko seperti ini dibagi menjadi empat jenis yaitu:

a. Pengungkapan Informsi yang tidak terotoritasis dan pencurian. Ketika suatu basis data dan perpustakaan peranti lunak tersedia bagi orang-orang yang seharusnya tidak memiliki akses, hasilnya adalah hilangnya informasi atau uang.
b. Penggunaan yang tidak terotorisasi. Penggunaan yang tidak terotorisasi terjadi ketika orang-orang yang biasanya tidak berhak menggunakan sumber daya perusahaan mampu melakukan hal tersebut.
c. Penghancuran yang tidak terotorisasi dan penolakan layanan. Seseorang dapat merusak atau menghancurkan peranti keras atau peranti lunak, sehingga menyebabkan operasional komputer perusahaan tersebut tidak berfungsi.
d. Modifikasi yang terotorisasi. Perubahan dapat dilakukan pada data, informasi, dan peranti lunak perusahaan yang dapat berlangsung tanpa disadari dan menyebabkan para pengguna output sistem tersebut mengambil keputusan yang salah.

F. PERSOALAN E-COMMERCE

E-Commerce memperkenalkan suatu permasalahan keamanan baru. Masalah ini bukanlah perllindungan data, informasi, dan piranti lunak, tetapi perlindungan dari pemalsuan kartu kredit.

Kartu Kredit "Sekali pakai"

Kartu sekali pakai ini bekerja dengan cara berikut: saat pemegang kartu ingin membeli sesuatu seccar online, ia akan memperleh angka yang acak dari situs web perusahaan kartu kredit tersebut. Angka inilah, dan bukannya nomor kartu kredit pelannggan tersebut, yang diberikan kepada pedadang e-commerce, yang kemudian melaporkannya ke perusahaan kartu kredit untuk pembayaran.

Praktik keamanan yang diwajibkan oleh Visa

Visa mengumumkan 10 pratik terkait keamanan yang diharapkan perusahaan ini untuk diikuti oleh peritelnya. Peritel yang memilih untuk tidak mengikuti praktik ini akan menghadapi denda, kehilangan keanggotaan dalam program visa, atau pembatasan penjualan dengan visa. Peritel harus :

1. Memasang dan memelihara firewall
2. Memperbaharui keamanan
3. Melakukan enkripsi data yang disimpan
4. Melakukan enkripsi pada data ynag dikirm
5. Menggunakan dan memperbaharui peranti lunak anti virus
6. Membatasi akses data kepada orang-orang yang ingin tahu
7. Memberikan id unik kepada setiap orang yang memiliki kemudahan mengakses data
8. Memantau akses data dengan id unik
9. Tidak menggunakan kata sandi default yang disediakan oleh vendor
10. Secara teratur menguji sistem keamanan

Selain itu, visa mengidentifikasi 3 praktik umum yang harus diikuti oleh peritel dalam mendapatkan keamanan informasi untuk semua aktivitas bukan hanya yang berhubungan dengan e-commerce:

1. Menyaring karyawan yang memiliki akses terhadap data
2. Tidak meninggalkan data atau komputer dalam keadaan tidak aman
3. Menghancurkan data jika tidak dibutuhkan lagi

G. MANAJEMEN RISIKO (MANAGEMENT RISK)

Manajemen Risiko merupakan satu dari dua strategi untuk mencapai keamanan informasi.Risiko dapat dikelola dengan cara mengendalikan atau menghilangkan risiko atau mengurangi dampaknya. Pendefenisian risiko terdiri atas empat langkah :

1. Identifikasi aset-aset bisnis yang harus dilindungi dari risiko
2. Menyadari risikonya
3. Menentukan tingkatan dampak pada perusahaan jika risiko benar-benar terjadi
4. Menganalisis kelemahan perusahaan tersebut

Tabel Tingkat Dampak dan Kelemahan

	Dampak Parah	Dampak Signifikan	Dampak Minor
Kelemahan Tingkat Tinggi	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Menengah	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Rendah	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Analisis kelemahan tidak dibutuhkan

Tingkat keparahan dampak dapat diklasifikasikan menjadi:

1. dampak yang parah (severe impact) yang membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan tersebut untuk berfungsi
2. dampak signifikan (significant impact) yang menyebabkan kerusakan dan biaya yang signifikan, tetapi perusahaan tersebut tetap selamat
3. dampak minor (minor impact) yang menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

Setelah analisis risiko diselesaikan, hasil temuan sebaiknya didokumentasikan dalam laporan analisis risiko. Isi dari laporan ini sebaiknya mencakup informasi berikut ini, mengenai tiap-tiap risiko:

1. diskripsi risiko
2. sumber risiko
3. tingginya tingkat risiko
4. pengendalian yang diterapkan pada risiko tersebut
5. para pemilik risiko tersebut
6. tindakan yang direkomendasikan untuk mengatasi risiko
7. jangka waktu yang direkomendasikan untuk mengatasi risiko

Jika perusahaan telah mengatasi risiko tersebut, laporan harus diselesaikan dengan cara menambahkan bagian akhir :

8. apa yang telah dilaksanakan untuk mengatasi risiko tersebut

KEBIJAKAN KEAMANAN INFORMASI

Suatu kebijakan keamanan harus diterapkan untuk mengarahkan keseluruhan program. Perusahaan dapat menerapkan keamanan dengan pendekatan yang bertahap, diantaranya:

a. Fase 1, Inisiasi Proyek. Membentuk sebuah tim untuk mengawas proyek kebijakan keamanan tersebut.
b. Fase 2, Penyusunan Kebijakan. Berkonsultasi dengan semua pihak yang berminat dan terpengaruh.
c. Fase 3, Konsultasi dan persetujuan. Berkonsultasi dengan manajemen untuk mendapatkan pandangan mengenai berbagai persyaratan kebijakan.

d. Fase 4, Kesadaran dan edukasi. Melaksanakan program pelatihan kesadaran dan edukasi dalam unit-unit organisasi.
e. Fase 5, Penyebarluasan Kebijakan. Kebijakan ini disebarluaskan ke seluruh unit organisasi dimana kebijakan tersebut dapat diterapkan.

Kebijakan Keamanan yang Terpisah dikembangkan untuk

a. Keamanan Sistem Informasi
b. Pengendalian Akses Sistem
c. Keamanan Personel
d. Keamanan Lingkungan Fisik
e. Keamanan Komunikasi data
f. Klasifikasi Informasi
g. Perencanaan Kelangsungan Usaha
h. Akuntabilitas Manajemen

Kebijakan terpisah ini diberitahukan kepada karyawan, biasanya dalam bentuk tulisan, dan melalui program pelatihan dan edukasi. Setelah kebijakan ini ditetapkan, pengendalian dapat diimplementasikan.

H. PENGENDALIAN

Pengendalian (control) adalah mekanisme yang diterapkan baik untuk melindungi perusahaan dari resiko atau untuk meminimalkan dampak resiko tersebut pada perusahaan jika resiko tersebut terjadi. Engendalian dibagi menjadi tiga kategori, yaitu :

1. PENGENDALIAN TEKNIS

Pengendalian teknis (*technical control*) adalah pengendalian yang menjadi satu di dalam system dan dibuat oleh para penyusun system selam masa siklus penyusunan system. Didalam pengendalian teknis, jika melibatkan seorang auditor internal didalam tim proyek merupakan satu cara yang amat baik untuk menjaga agar pengendalian semacam ini menjadi bagian dari desain system. Kebanyakan pengendalian keamanan dibuat berdasarkan teknologi peranti keras dan lunak.

1. Pengendalian Akses

Dasar untuk keamanan melawan ancaman yang dilakukan oleh orang-orang yang tidak diotorisasi adalah pengendalian akses. **Alasannya sederhana:** Jika orang yang tidak diotorisasi tidak diizinkan mendapatkan akses terhadap sumber daya informasi, maka pengrusakan tidak dapat dilakukan.

Pengendalian akses dilakukan melalui proses tiga tahap yang mencakup:

1. **Identifikasi pengguna.** Para pengguna pertama-tama mengidentifikasi diri mereka dengan cara memberikan sesuatu yang mereka *ketahui*, misalnya kata sandi. Identifikasi dapat pula mencakup *lokasi* pengguna, seperti nomor telepon atau titik masuk jaringan.
2. **Autentifikasi pengguna.** Setelah identifkasi awal telah dilakukan, para pengguna memverikasi hak akses dengan cara memberikan sesuatu yang mereka *miliki*, seperti *smart card* atau tanda tertentu atau *chip* identifikasi. Autentifikasi pengguna dapat juga dilaksanakan dengan cara memberikan sesuatau yang menjadi identitas diri, seperti tanda tangan atau suara atau pola suara.

3. **Otorisasi pengguna.** Setelah pemeriksaan identifikasi dan autentifikasi dilalui, seseorang kemudian dapat mendapatkan otorisasi untuk memasuki tingkat atau derajat penggunaan tertentu. Sebagai contoh, seorang pengguna dapat mendapatkan otorisasi hanya untuk membaca sebuah rekaman dari suatu *file,* sementara pengguna yang lain dapat saja memiliki otorisasi untuk melakukan perubahan pada *file* tersebut.

Identifkasi dan autentifikasi memanfaatkan **profil pengguna (user profile),** atau deskripsi pengguna yang terotorisasi. Otorisasi memanfaatkan **file pengendalian akses (acess control file)** yang menentukan tingkat akses yang tersedia bagi tiap pengguna.

Setelah para pengguna memenuhi syarat tiga fungsi pengendalian kases, mereka dapat menggunakan sumber daya informasi yang terdapat di dlaam batasan file pengendalian akses. Pencatatan audit yang berbasis komputer terus dilakukan pada semua aktivitas pengendalian akses, seperti tanggal dan waktu serta identifikasi terminal, dan digunakan untuk mempersiapkan laporan keuangan.

2. System Deteksi Gangguan

Logika dasar dari system deteksi gangguan adalah mengenali upaya pelanggaran keamanan *sebelum* memiliki kesempatan untuk melakukan perusakan. Salah satu contoh yang baik adalah **peranti lunak proteksi virus (*virus protection software*)** yang telah terbukti efektif melawan virus yang terkirim melalui *e-mail*. Peranti lunak tersebut mengidentifikasi pesan pembawa virus dan memperingatkan si pengguna.

Contoh deteksi pengganggu yang lain adalah peranti lunak yang ditujukan untuk mengidentifikasikan calon pengganggu sebelum memiliki kesempatan untuk membahayakan. **Peralatan prediksi ancaman dari dalam (*insider threat prediction tool*)** telah disusun sedemikian rupa sehingga dapat mempertimbangkan karakteristik seperti posisi seseorang di dalam perusahaan, akses ke dalam data yang sensitive, kemampuan untuk mengubah komponen peranti keras, jenis aplikasi yang digunakan, *file* yang dimilki, dan penggunaan protocol jaringan tertentu. Hasil pembuatan profilan seperti ini, yang beberapa berbentuk kuantitatif, dapat mengklasifikasikan ancaman internal ke dalam kategori seperti *ancaman yang disengaja, potensi ancaman kecelakaan, mencurigakan, dan tidak berbahaya.*

3. Firewall

Sumber daya komputer selalu berada dalam resiko jika terhubung ke jaringan. Salah satu pendekatan keamanan adalah secara fisik memisahkan situs Web perusahaan dengan jaringan internal perusahaan yang berisikan data sensitive dan system informasi. Cara lain adalah menyediakan kata sandi kepada mitra dagang yang memungkinkannya memasuki jaringan internal dari Internet.

Pendekatan ketiga adalah membangun dinding pelindung atau *firewall*. *Firewall* berfungsi sebagai penyaring dan penghalang yeng membatasi aliran data ked an dari perusahaan tersebut dan Internet. Konsep dibalik *firewall* adalah dibuatnya suatu pengaman untuk semua komputer pada jaringan perusahaan dan bukannya pengaman terpisah untuk masing-masing computer. Beberapa perusahaan yang menawarkan peranti lunak antivirus (seperti McAfee di www.mcafee.com dan www.norton.com) sekarang memberikan peranti lunak *firewall* tanpa biaya ekstra dengan pembelian produk antivirus mereka.

Ada tiga jenis firewall, yaitu:

1. **Firewall Penyaring Paket.** *Router* adalah alat jaringan yang mengarahkan aliran lalu lintas jaringan. Jika *router* diposisikan antara Internet dan jaringan internal, maka router dapat berlaku sebagai *firewall*. *Router* dilengkapi dengan table data dan alamat-alamat IP yang menggambarkan kebijakan penyaringan. Untuk masing-masing transmisi, *router* mengakses table-tabelnya dan memungkinkan hanya beberapa jenis pesan dari beberapa lokasi Internet (alamat IP) untuk lewat. Alamat IP (*IP Address*) adalah serangkaian empat angka (masing-masing dari 0 ke 255) yang secara unik mengidentifikasi masing-masing computer yang terhubung dengan Internet. Salah satu keterbasan *router* adalah *router* hanya merupakan titik tunggal keamanan, sehingga jika hacker dapat melampuinya perusahaan tersebut bisa mendapatkan masalah. "IP *spoofing",* yaitu menipu table akses *router*, adalah dalah satu metode yang digunakan untuk pembajak untuk menipu *router*.
2. **Firewall Tingkat Sirkuit.** Salah satu peningkatan keamanan dari *router* adalah *firewall* tingkat sirkuit yang terpasang antara Internet dan jaringan perusahaan tapi lebih dekat dengan medium komunikasi (sirkuit) daripada *router*. Pendekatan ini memungkinkan tingkat autentifikasi dan penyaringan yang tinggi, jauh lebih tinggi dibandingkan *router*. Namun, keterbatasan dari titik tunggal keamanan tetap berlaku.
3. **Firewall Tingkat Aplikasi.** *Firewall* ini berlokasi antara *router* dan computer yang menajlankan aplikasi tersebut. Kekuatan penuh pemeriksaan keamanan tambahan dapat dilakukan. Setelah permintaan diautentifikasi sebagai permintaan yang berasal dari jaringan yang diotorisasi (tingkat sirkuit) dan dari computer yang diotorisasi (penyaringan paket), aplikasi tersebut dapat memnita informasi autentifikasi yang lebih jauh seperti menanyakan kata sandi sekunder, mengonfirmasikan identitas, atau bahkan memeriksa apakah permintaan tersebut berlangsung selama jam-jam kerja biasa. Meskipun merupakan jenis *firewall* yang paling efektif, *firewall* ini cenderung untuk mengurangi akses ke sumber daya. Masalah lain adalah seorang programmer jaringan harus penulis kode program yang spesifik untuk masing-masing aplikasi dan mengubah kode tersebut ketika aplikasi ditambahkan, dihapus, dimodifikasi.
4. Pengendalian Kriptografis

   Data dan informasi yang tersimpan dan ditransmisikan dapat dilindungi dari pengungkapan yang tidak terotorisasi dengan kriptografi, yaitu penggunaan kode yang menggunakan proses-proses matematika. Data dan informasi tersebut dapat dienkripsi dalam penyimpanan dan juga ditransmisikan kedalam jaringan. Jika seseorang yang tidak memiliki otorisasi memperoleh akses enkripsi tersebut akan membuat data dan informasi yang dimaksud tidak berarti apa-apa dan mencegah kesalahan penggunaan.

   Popularitas kriptografis semakin meningkat karena *e-commerce,* dan produk khusus ditujukan untuk meningkatkan keamanan *e-commerce* telah dirancang. Salah satunya adalah SET (*Secure Electronic Transactions*), yang ,melakukan pemeriksaan keamanan menggunakan tanda tangan digital. Tanda tangan ini dikeluarkan kepada orang-orang yang dapat berpartisispasi dalam transaksi *e-commerce* – pelanggan, penjual, dan institusi keuangan. Dua tanda tangan biasanya digunakan menggantikan nomor kartu kredit.

5. Pengendalian Fisik

Peringatan pertama terhadap gangguan yang tidak terotorisasi adalah mengunci pintu ruangan computer. Perkembangan seterusnya menghasilkan kunci-kunci yang lebih canggih yaitu dibuka dengan cetakan telapak tangan dan cetakan suara, serta kamera pengintai dan alat penjaga keamanan. Perusahaan dapat melaksanakan pengendalian fisik hingga pada tahap tertinggi dengan cara menempatkan pusat komputernya ditempat terpencil yang jauh dari kota dan jauh dari wilayah yang sensitive terhadap bencana alam seperti gempa bumi, banjir, dan badai.

6. Meletakkan Pengendalian Teknis Pada Tempatnya

Anda dapat melihat dari daftar penjang pengendalian teknis ini (dan tidak semuanya dicantumkan), bahwa teknologi telah banyak digunakan untuk mengamankan informasi. Pengendalian teknis dikenal sebagai yang terbaik untuk keamanan. Perusahaan biasanya memilih dari daftar ini dan menerapkan kombinasi yang dianggap menawarkan pengaman yang paling realisitis.

2. PENGENDALIAN FORMAL

Pengendalian formal mencakup penentuan cara berperilaku, dokumentasi prosedur dan praktik yang diharapkan, dan pengawasan serta pencegahanperilaku yang berbeda dari panduan yang berlaku. Pengendalian ini bersifat formal karena manajemen menghabiskan banyak waktu untuk menyusunnya, mendokumentasikannya dalam bentuk tulisan, dan diharapkan dapat berlaku dalam jangka panjang.

3. PENGENDALIAN INFORMAL

Pengendalian informal mencakup program-program pelatihan dan edukasi serta program pembangunan manajemen. Pengendalian ini ditujukan untuk menjaga agar para karyawan perusahaan memahami serta mendukung program keamanan tersebut.

MENCAPAI TINGAKAT PENGENDALIAN YANG TEPAT

Ketiga jenis pengendalian – teknis, formal, dan informal – mengharuskan biaya. karena bukanlah merupakan praktik bisnis yang baik untuk mengahabiskan lebih banyak uang pada pengendalian dibandingkan biaya yang diharapkan dari resiko yang akan terjadi, maka pengendalian harus ditetapkan pada tingkat yang sesuai. Dengan demikian, keputusan untuk mengendalikan pada akhirnya dibuat berdasarkan biaya versus keuntungan, tapi dalam beberapa industry terdapat pula pertimbangan-pertimbangan lain.

DUKUNGAN PEMERINTAH DAN INDUSTRI

Beberapa organisasi pemerintahan dan internasional telah menentukan standar-standar yang ditujukan untuk menjadi panduan organisasi yang ingin mendapatkan keamanan informasi. Beberapa standar ini berbentuk tolak ukur, yang telah diidentifikasi sebelumnya sebagai penyedia strategi alternative untuk manajemen resiko. Organisasi tidak diwajibkan mengikuti standar ini, namun standar ini ditujukan untuk memberikan bantuan kepada perusahaan dalam menentukan tingkat target keamanan. Berikut ini adalah beberapa contohnya :

- **BS7799 Milik Inggris**
- **BSI IT Baseline Protection Manual**
- **COBIT**
- **GASSP (*Generally Accepted System Security Principles*)**

- **ISF Standard of Good Practice**

Tidak ada satupun dari standar-standar ini yang menawarkan cakupan yang menyeluruh dari masalah ini. Namun, jika disatukan, standar-standar tersebut menjadi dasar yang baik untuk diikuti perusahaan dalam menentukan kebijakan keamanan informasinya sendiri yang mendukung budaya organisasi tersebut.

PERATURAN PEMERINTAH

Pemerintah baik di Amerika Serikat maupun Inggris telah menentukan standard an menetapkan standardan menetapkan peraturan yang ditujukan untuk menaggapi masalah pentingnya keamanan informasi yang makin meningkat, terutama setelah peristiwa 9/11 dan semakin meluasnya internet serta peluang terjadinya kejahatan computer. Beberapa dioantaranya adalah :

- **Standar Keamanan Komputer Pemerintah Amerika Serikat**
- **Undang-undang Anti Terorisme, Kejahatan, dan Keamanan Inggris (ATCSA) 2001**
- **STANDAR INDUSTRI**

The Center for Internet Security (CIS) adalah organisasi nirlaba yang didedikasikan untuk membantu para mengguna computer guna membuat system mereka lebih aman. Bantuan diberikan melalui dua produk – CIS Benchmark dan CIS Scoring Tools.

SERTIFIKASI PROFESIONAL

Mulai tahun 1960-an,profesi TI mulai menawarkan program sertifikasi. Tiga contoh berikut mengilustrasikan cakupan dari program-program ini.

- **Asosiasi Audit Sistem dan Pengendalian**
- **Konsersium Sertifikasi Keamanan Sistem Informasi Internasional**
- **Institute SANS**

MELETAKKAN MANAJEMEN KEAMANAN INFORMASI PADA TEMPATNYA

Perusahaan harus mencanangkan kebijakan manajemen keamanan informasi sebelum menempatkan pengendalian yang didasarkan atas identifikasi ancaman dan risiko ataupun atas panduan yang diberikan oleh pemerintah atau asosiasi industri. Perusahaan harus mengimplementasikan gabungan dari pengendalian teknis, formal, dan informal yang diharapkan untuk menawarkan tinngkat keamanan yang diinginkan pada batasan biaya yang ditentukan dan sesuai dengan pertimbangan lain yang membuat perusahaan dan sistemnya mamapu berfungsi secara efektif.

MANAJEMEN KEBERLANGSUNGAN BISNIS

Manajemen keberlangsungan bisnis (bussines continuity management – BCM) adalah aktivitas yang ditujukan untuk menentukan operasional setelah terjadi gangguang sistem informasi. Pada tahun awal penggunaan komputer, aktivitas ini disebut perencanaan bencana (disaster planing), namun istilah yang lebih positif perencanaan kontijensi (contigency plan), menjadi populer. Elemen penting dalam perenccanaan kontijensi adalah rencana kontijensi, yang merupakan dokumen tertulis, formal yang menyebutkan secara detail tindakan-tindakan yang harus dilakukan jika terjadi gangguan, atau ancaman gangguan, pada operasi komputasi perusahaan.

Banyak perusahaan telah menemukan bahwa, dibanding sekedar mengandalkan, satu rencana kontijensi besar, pendekatan yang terbaik adalah merancang beberapa sub rencana yang menjawab beberapa kontijensi yang spesifik. Sub rencana yang umum mencakup :

Rencana darurat (Emergency plan). Rencana darurat menyebutkan cara-cara yang akan menjaga keamanan karyawan jika bencana terjadi. Cara-cara ini mencakup sistem alarm, prosedur evakuasi dan sistem pemadaman api.

Rencana cadangan. Perusahaan harus mengatur agar fasilitas komputer cadangan tersedia seandainya fasilitas yang biasa hancur atau rusak sehingga tidak digunakan. Cadangan ini dapat diperoleh melalui kombinasi dari :

1. Redudansi. Peranti keras, peranti lunak dan data di duplikasikan sehingga jika satu set tidak dapat dioperasikan, set cadangannya dapat meneruskan proses.
2. Keberagaman. Sumber daya informasi tidak dipasang pada tempat yang sama, komputer dibuat terpisah untuk wilayah operasi yang berbeda-beda.
3. Mobilitas. Perusahaan dapat membuat perjanjian dengan para pengguna peralatan yang sama sehingga masing-masing perusahan dapat menyediakan cadangan kepada yang lain jika terjadi bencana besar. Pendekatan yang lebih detail adalah membuat kontrak dengan jasa pelayanan cadangan *hot site dan cold site*. Hot site adalah fasilitas komputer lengkap yang disediakan oleh pemasok untuk pelanggannya untuk digunakan jika terdapat situasi darurat. Cold site hanya mencakup fasilitas bangunan namun tidak mencakup fasilitas komputer.

Rencana catatan penting. Catatan penting (vital records) perusahaan adalah dokumen kertas, microform dan media penyimpanan optimis dan magnetis yang penting untuk meneruskan bisnis perusahaan tersebut. Rencana catatan penting (vital records plan) menentukan cara bagaimna catatan penting tersebut harus dilindungi. Selain menjaga catatan tersebut di situs komputer, cadanan harus disimpan dilokasi. Semua jenis catatan dapat secara fisik dipindahkan ke lokasi terpencil tersebut, namun catatan komputer dapat ditransmisikan secara elektronik.

MELETAKKAN MANAJEMEN KEBERLANGSUNGAN BISNIS PADA TEMPATNYA

Manajemen keberlangsungan bisnis merupakan salah satu bidang pengunaan komputer dimana kita dapat melihat perkembangan besar. Banyak upaya telah dilaksanakan untuk mengembangkan perencanaan kontijensi, dan banyak informasi serta bantuan telah tersedia. Tersedia pula rencana dalam paket sehingga perusahaan dapat mengadaptasinya ke dalam kebutuhan khususnya. Sistem komputer TAMP memasarakan sistem pemulihan bencana (disaster recovery system – DRS) yang mencakup sistem manajemen basis dasa, instruksi, dan perangkat yang dapat digunakan untuk mempersiapkan rencana pemulihan. Panduan dan garis besar tersedia bagi perusahaan untuk digunakan sebagai titik awal atau tolak ukur.