Universitas Bina Darma

FIND US FOR QUALITY

KEAMANAN INFORMASI

Tujuan Pengajaran

- Memahami kebutuhan organisasi akan keamanan dan pengendalian.
- Memahami bahwa keamanan informasi berkaitan dengan keamanan semua sumber daya informasi, bukan hanya piranti keras dan data.
- Memahami tiga tujuan utama keamanan informasi.
- Memahami bahwa manajemen keamanan informasi terdiri atas dua area: manajemen keamanan informasi *(information security management-ISM)* dan manajemen keberlangsungan bisnis *(business continuity management-BCM).*
- Melihat hubungan yang logis antara ancaman, risiko dan pengendalian.
- Memahami apa saja ancaman keamanan yang utama.
- Memahami apa saja risiko keamanan yang utama.

Lanjutan....

- Mengenali berbagai kekhawatiran keamanan e-commerce dan bagaimana jaminan perusahaan-perusahaan mengatasinya.
- Mengenali cara formal melakukan manajemen risiko.
- Mengetahui proses implementasi kebijakan keamanan informasi.
- Mengenali cara-cara pengendalian keamanan yang populer.
- Mengetahui tindakan-tindakan pemerintah dan kalangan industri yang mempengaruhi kemanan informasi.
- Mengetahui cara mendapatkan sertifikasi profesional dalam keamanan dan pengendalian.
- Mengetahui jenis-jenis rencana yang termasuk dalam perencanaan kontijensi.

Kebutuhan Organisasi Akan Keamanan dan Pengendalian

- Pengalaman yang menginspirasi kalangan industri:
  - Meletakkan penjagaan keamanan untuk menghilangkan atau mengurangi kemungkinan kerusakan.
  - Menyediakan organisasi dengan kemampuan untuk melanjutkan kegiatan operasional setelah terjadi gangguan.
- Patriot Act and the Office of Homeland Security
  - Isu keamanan vs. hak-hak individual.
  - Isu keamanan vs. ketersediaan (i.e., HIPPA).

Keamanan Informasi

- **System security** diperluas tidak terbatas pada hardware, data, software, computer facilities, and personnel.
- **Information security** digunakan untuk mendeskrispsikan perlindungan baik peralatan komputer dan non-komputer, fasilitas, data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang.
  - Mencakup peralatan seperti mesin photocopy dan mesin fax serta semua jenis media, termasuk dokumen kertas.

Tujuan Keamanan Informasi

- Keamanan informasi ditujukan untuk mencapai tiga tujuan utama:
  - **Kerahasiaan:** melindungi data dan informasinya dari pengungkapan kepada orang-orang yang tidak berwenang.
  - **Ketersediaan:** menyediakan data dan informasi sedia bagi pihak-pihak yang memiliki wewenang untuk menggunakannya.
  - **Integritas:** informasi harus memberikan representasi akurat atas sistem phisik yang direpresentasikan.
- Sistem informasi perusahaan seharusnya melindungi dari penyalahgunaan data dan informasi, menjamin ketersediaan pada pengguna yang sah, ditunjukkan secara terpercaya dan akurat.

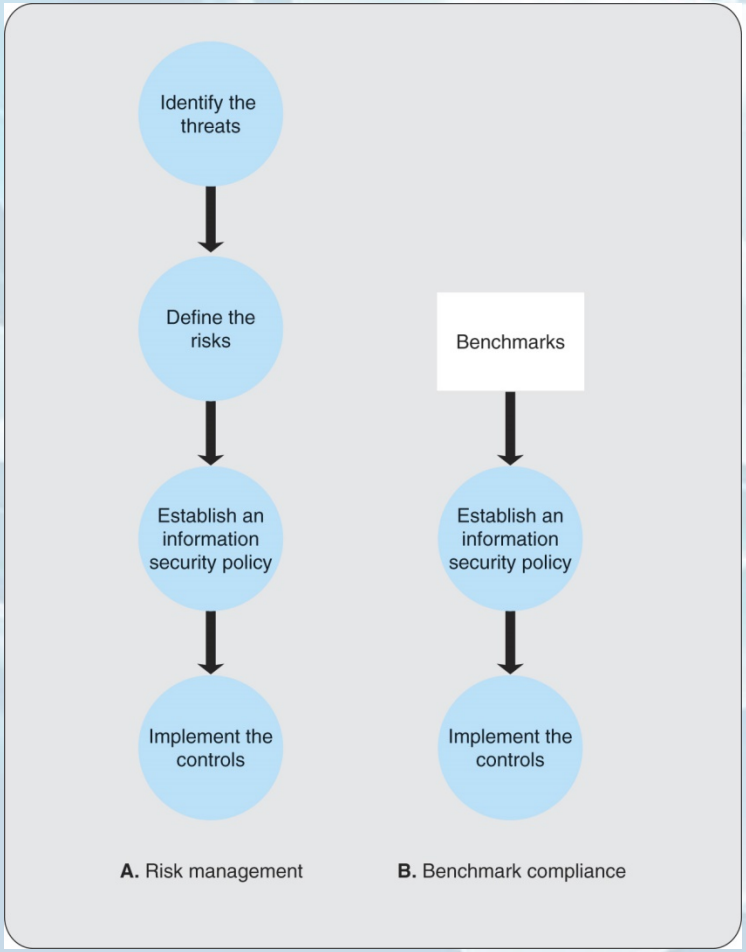
Manajemen Keamanan Informasi

- **Information security management** (**ISM**) aktivitas untuk menjaga agar sumber daya informasi tetap aman.
- **Business continuity management** (**BCM**) aktivitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah adanya bencana.
- **Corporate information systems security officer** (**CISSO**) bertanggung jawab atas keamanan sistem informasi perusahaan tersebut.
- **Corporate information assurance officer** (**CIAO**) melapor kepada CEO dan mengelola unit penjagaan informasi.

Manajemen Keamanan Informasi

- Menitikberatkan dengan formulasi kebijakan keamanan informasi perusahaan.
- **Risk management** pendekatan ini dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.
- **Information security benchmark** adalah tingkat keamanan yang disarankan pada keadaan normal harus menawarkan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi.
  - *Tolok ukur adalah tingkat kinerja yang disarankan.*
  - Ditetapkan oleh pemerintah dan asosiasi industri.
  - Mencerminkan komponen-komponen program keamanan informasi yang baik menurut otoritas-otoritas tersebut.
- **Benchmark compliance** dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolok ukur tersebut.

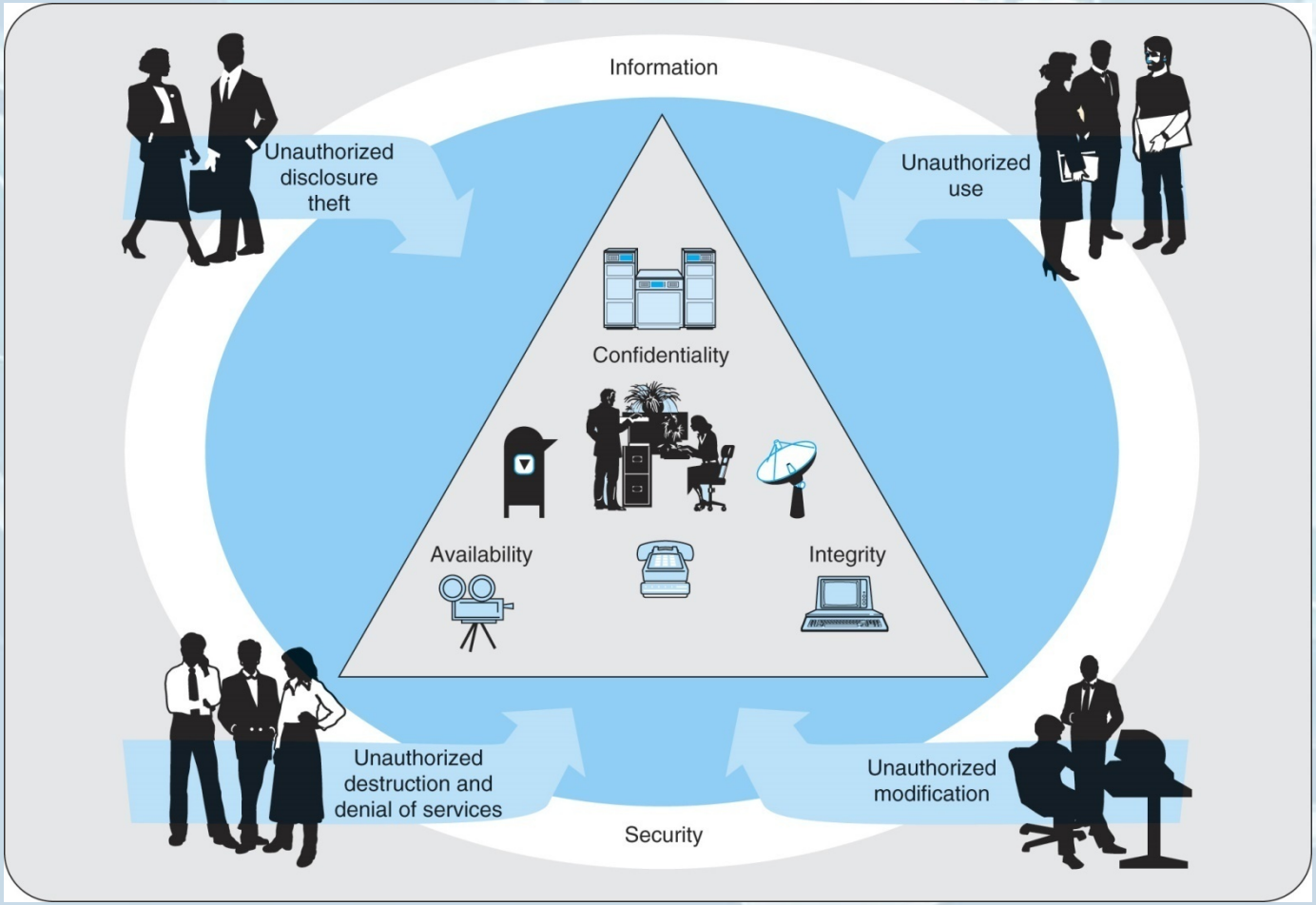
Figure 9.1 Information Security Management (ISM) Strategies



Ancaman

- **Information security threat** adalah orang, organisasi, mekanisme atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan.
- *Ancaman internal dan eksternal*
  - Ancaman internal meliputi bukan hanya karyawan perusahan tetapi juga pekerja temporer, konsultan, kontraktor dan bahkan mitra bisnis perusahaan tersebut.
  - As high as 81% of computer crimes have been committed by employees.
  - Ancaman Internal diperkirakan menghasilkan kerusakan yang secara potensial lebih serius jika dibandingkan dengan ancaman eksternal, dikarenakan pengetahuan ancaman internal yang lebih mendalam akan sistem tersebut.
- *Kecelakaan dan tindak kesengajaan*

Figure 9.2 Unauthorized Acts Threaten System Security Objectives



Jenis-jenis ancaman

- **Malicious software** (**malware**) terdiri atas program-program yang lengkap atau segmen-segmen kode yang dapat menyerang suatu sistem dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemilik sistem.
- **Virus** adalah program komputer yang dapat mereplikasikan dirinya sendiri tanpa dapat diamati oleh si pengguna dan menempelkan salinan dirinya pada program-program dan *boot sector* lain.
- **Worm** (cacing) tidak dapat mereplikasi dirinya sendiri di dalam sistem, tapi dapat menyebarkan salinannya melalui email.
- **Trojan horse** mendistribusikan dirinya sendiri; si pengguna menyebarkan sebagai perangkat keras. Tidak dapat mereplikasi dirinya sendiri.
- **Adware** memunculkan pesan-pesan yang mengganggu.
- **Spyware** mengumpulkan data dari mesin pengguna.

Risiko

- **Information security risk** potensi output yang tidak diharapkan dari pelanggaran keamanan informasi.
  - Semua risiko mewakili tindakan yang tidak terotorisasi.
- *Pengungkapan informasi dan ancaman yang tidak terotorisasi.*
- *menggunakan yang tanpa otorisasi.*
- *Penghancuran dan penolakan layanan tanpa otorisasi.*
- *Modifikasi tanpa otorisasi.*

Persoalan e-commerce

- *Disposable credit card* (AMEX) – tindakan yang ditujukan bagi 60 hingga 70 persen konsumen yang mengkhawatirkan pemalsuan kartu kredit dari penggunaan internet.
- *Visa mengumumkan 10 praktek terkait keamanan yang diharapkan perusahaan ini untuk diikuti oleh para peritelnya.*
- *Cardholder Information Security Program* (*CISP*) ditujukan pada peritel; dengan tujuan untuk menjaga data pemegang kartu.

Manajemen Risiko

- Pendefinisian risiko terdiri atas empat langkah:
  - Identifikasi aset-aset bisnis yang harus dilindungi dari risiko.
  - Menyadari risikonya.
  - Menentukan tingkatan dampak pada perusahaan jika risiko benar-benar terjadi.
  - Menganalisis kelemahan perusahaan tersebut.
- Tingkat keparahan dampak dapat diklasifikasikan menjadi:
  - **Severe impact** (dampak yang parah) membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan untuk beroperasi.
  - **Significant impact** (dampak signifikan) menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.
  - **Minor impact** menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

Table 9.1 Degree of Impact and Vulnerability Determine Controls

Degree of Impact and Vulnerability Determine Controls

	Severe Impact	Significant Impact	Minor Impact
High Vulnerability	Conduct vulnerability analysis. Must improve controls.	Conduct vulnerability analysis. Must improve controls.	Vulnerability analysis unnecessary.
Medium Vulnerability	Conduct vulnerability analysis. Should Improve controls.	Conduct vulnerability analysis. Should Improve controls.	Vulnerability analysis unnecessary.
Low Vulnerability	Conduct vulnerability analysis. Keep controls intact.	Conduct vulnerability analysis. Keep controls intact.	Vulnerability analysis unnecessary.

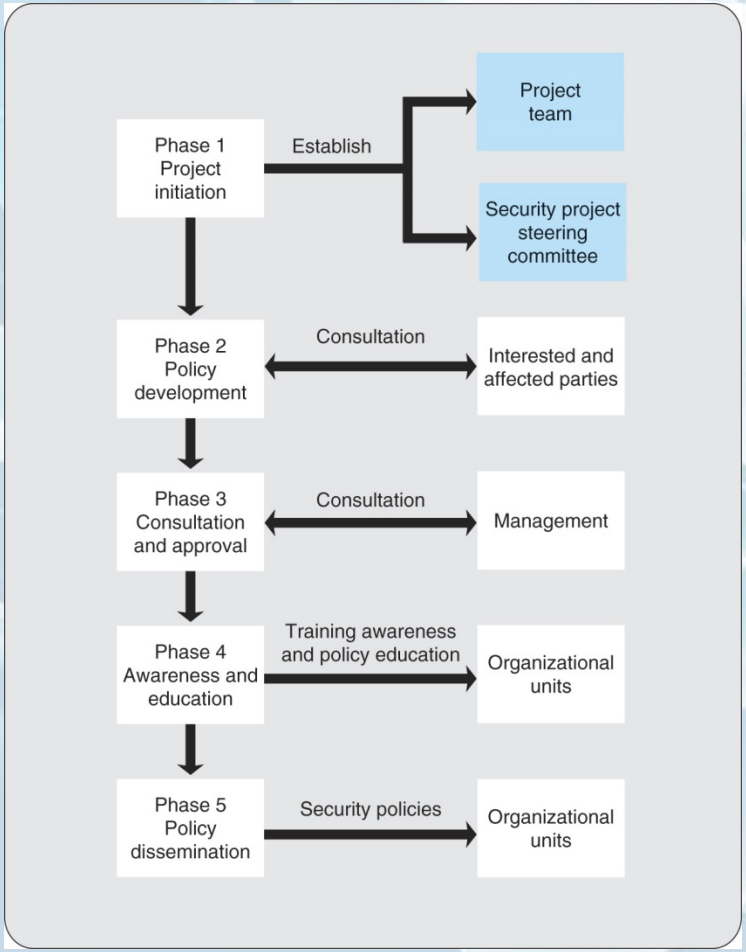
laporan Analsis Risiko

- Hasil temuan sebaiknya didokumentasikan dalam laporan analisis risiko. Isi laporan sebaiknya mencakup informasi berikut ini, mengenai tiap-tiap risiko:
  - Deskripsi risiko
  - Sumber risiko
  - Tingginya tingkat risiko
  - Pengendalian yang diterapkan pada risiko tersebut
  - Para pemilik risiko tersebut
  - Tindakan yang direkomendasikan untuk mengatasi risiko
  - Tindakan yang direkomendasikan untuk mengatasi risiko
  - Jangka waktu yang direkomendasikan untuk mengatasi risiko

Kebijakan Keamanan Informasi

- Lima fase implementasi kebijakan keamanan:
  - Phase 1: Inisiasi proyek.
  - Phase 2: Penyusunan kebijakan.
  - Phase 3: Konsultasi dan persetujuan.
  - Phase 4: Kesadaran dan edukasi.
  - Phase 5: Penyebarluasan kebijakan.

Figure 9.3 Development of Security Policy



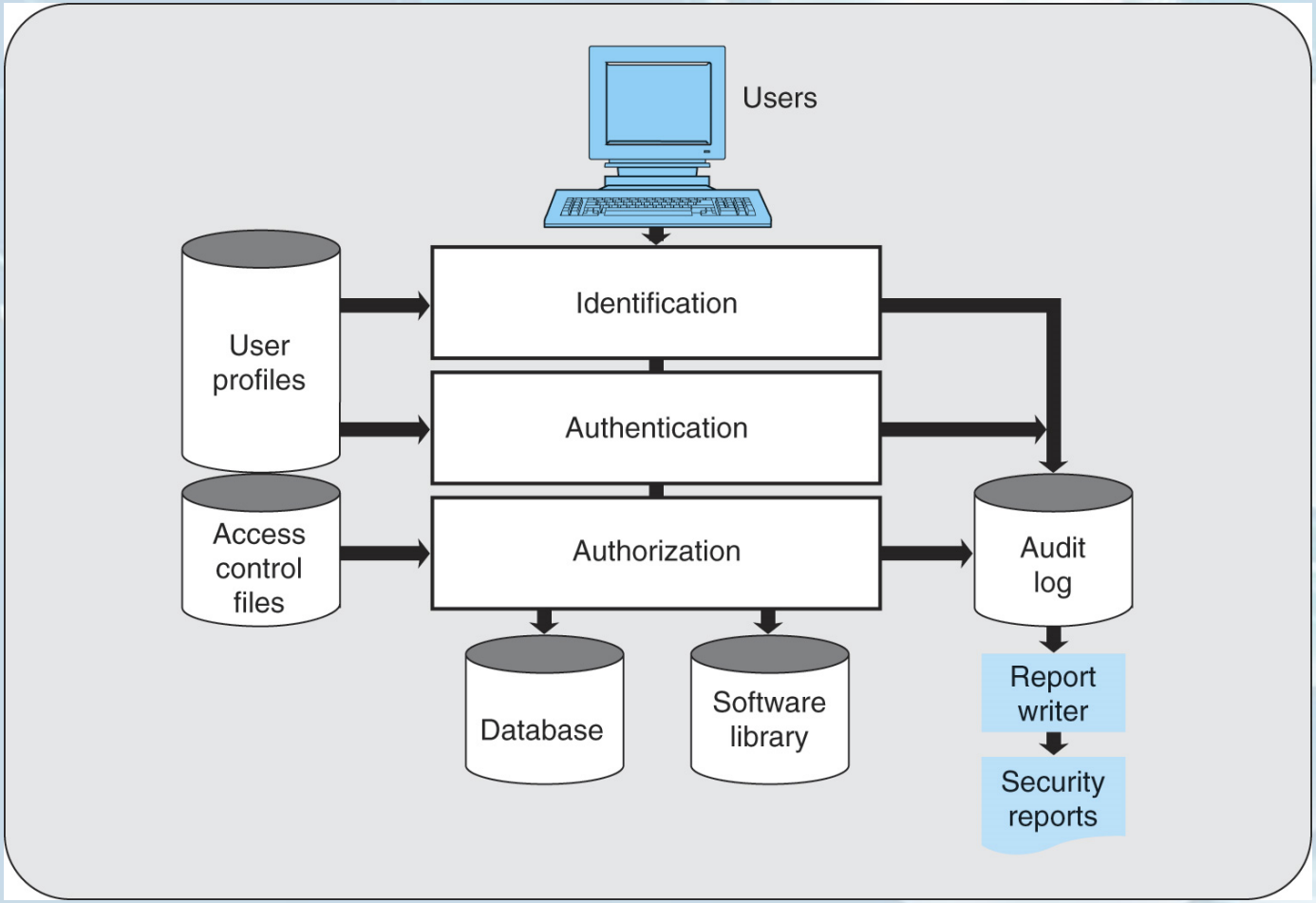
Pengendalian

- **Control** (pengendalian) adalah mekanisme yang diterapkan baik untuk melindungi perusahaan dari risiko atau untuk meminimalisasi dampak risiko tersebut pada perusahaan jika risiko tersebut terjadi.
- **Technical controls** (pengendalian teknis) adalah pengendalian yang menjadi satu dalam sistem dan dibuat oleh para penyusun sistem selama masa siklus penyusunan sistem.
  - Melibatkan seorang auditor internal di dalam tim proyek.
  - Berdasarkan teknologi perangkat keras dan perangkat lunak.

Pengendalian Akses

- **Access control** dasar untuk keamanan melawan ancaman yang dilakukan oleh orang-orang tanpa otorisasi adalah pengendalian akses.
- Pengendalian akses dilakukan melalui proses tiga tahap yang mencakup:
  - *Identifikasi pemakai.*
  - *Otentifikasi pemakai.*
  - *Otorisasi pemakai.*
- **User profiles**-deskripsi pengguna yang terotorisasi; digunakan dalam identifikasi dan otorisasi.

Figure 9.4 Access Control Functions



Source: Ken Cutler, "Hackers, Viruses, Thieves, and Other Threats to Your Information Assets," in *Computer Security Seminar Course Material* (New York: ACM, 1991).

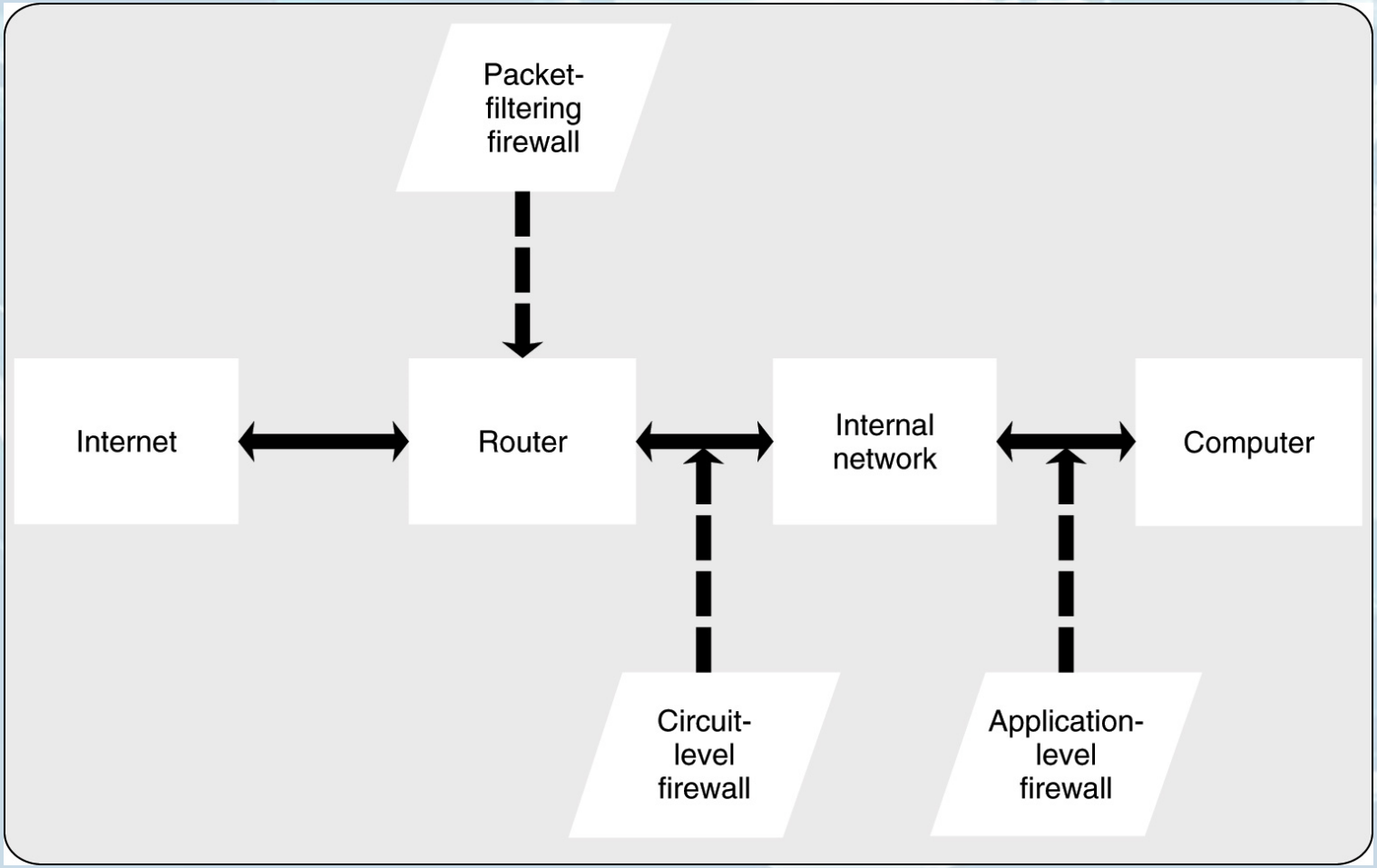
Lanjutan …

- **Intrusion detection systems** (**IDS**) sistem deteksi gangguan, mengenali upaya pelanggaran keamanan sebelum memiliki kesempatan untuk melakukan perusakan.
- Virus protection software telah terbukti efektif melawan virus yang terkirim melalui e-mail.
  - Mengidentifikasi pesan pembawa virus dan memperingatkan si pemakai.
- **Inside threat prediction tools** peralatan prediksi ancaman dari dalam, mengklasifikasikan ancaman internal dalam kategori sebagai berikut:
  - Possible intentional threat (ancaman yang disengaja)
  - Potential accidental threat (potensi ancaman kecelakaan).
  - Suspicious (mencurigakan).
  - Harmless (tidak berbahaya).

Firewalls

- **Firewall** berfungsi sebagai penyaring dan penghalang untuk membatasi aliran data dari dan ke perusahaan tersebut melalui internet. Tiga jenis firewalls adalah:
- **Packet-filtering** are routers itu dilengkapi tabel data alamat-alamat IP yang menggambarkan kebijakan penyaringan. Jika diposisikan antara internet dan jaringan internal, router tersebut dapat berlaku sebagai *firewall.*
  - *Router* adalah jaringan yang mengarahkan aliran lalu lintas jaringan.
  - **IP address** is a set of four numbers (each from 0 to 255) that uniquely identify each computer connected to the Internet.
- **Circuit-level firewall** yang terpasang antara internet dan jaringan perusahaan tapi lebih dekat dengan medium komunikasi (sirkuit) daripada router.
  - Memungkinkan tingkat otentifikasi dan penyaringan yang tinggi.
- **Application-level firewall** berlokasi diantara router dan komputer yang menjalankan aplikasi tersebut.
  - Kekuatan penuh pemeriksaan keamanan tambahan dapat dilakukan.

Figure 9.5 Location of Firewalls in the Network



Pengendalian Kriptografis

- **Cryptography** penggunaan kode seperti pada proses-proses matematika.
- Data dan informasi tersebut dapat dienkripsi dalam penyimpanan dan juga ditransmisikan ke dalam 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.
- Special protocols such as **SET** (Secure Electronic Transactions) melakukan pemeriksaan keamanan menggunakan tanda tangan digital.
- Ekspor teknologi enkripsi ke Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.
- *Pengendalian fisik,* peringatan pertama terhadap gangguan yang tidak terotorisasi adalah mengunci pintu ruangan komputer.
  - Menempatkan pusat komputernya di tempat terpencil yang jauh dari wilayah yang sensitif terhadap bencana alam seperti gempa bumi, banjir dan badai.

Pengendalian Formal

- **Formal controls** mencakup penentuan cara berperilaku, dokumentasi prosedur dan praktek yang diharapkan dan pengawasan serta pencegahan perilaku yang berbeda dari panduan yang berlaku.
  - Manajemen menghabiskan banyak waktu untuk menyusunnya.
  - Mendokumentasikannya dalam bentuk tulisan.
  - Diharapkan untuk berlaku dalam jangka panjang.
- Manajemen puncak harus berpartisipasi secara aktif dalam menentukan dan memberlakukannya.

Pengendalian Informal

- Pendidikan.
- Program pelatihan.
- Program pengembangan manajemen.
- Pengendalian ini ditujukan untuk menjaga agar para karyawan perusahaan memahami serta mendukung program keamanan tersebut.
- Good business practice bukanlah merupakan praktek bisnis yang baik untuk menghabiskan lebih banyak uang pada pengendalian dibandingkan biaya yang diharapkan dari risiko yang terjadi.
  - Maka pengendalian harus ditetapkan pada tingkatan yang sesuai.

Dukungan Pemerintah dan Industri

- **United Kingdom's BS7799.** standar Inggris menentukan satu set pengendalian dasar standar ini pertama kali dipublikasikan oleh British Standards Institute pada tahun 1995, kemudian dipublikasikan oleh International Standars Organization sebagai ISO 17799 pada tahun 2000 dan dibuat tersedia bagi para pengadopsi potensial secara online pada tahun 2003.
- **BSI IT Baseline Protection Manual.** Pendekatan baseline ini juga diikuti oleh German Bundesamt fur Sicherheit in der Informationstechnik (BSI). baselines ini ditujukan untuk memberikan keamanan yang cukup jika yang menjadi tujuan adalah kebutuhan proteksi normal. baselines dapat juga digunakan sebagai landasan perlindungan dengan kadar yang lebih tinggi jika dibutuhkan.
- **COBIT.** COBIT, dari the Information Systems Audit and Control Association and Foundation (ISACAF), berfokus pada proses yang dapat diikuti perusahaan dalam menyusun standar, dengan berfokus pada penulisan dan pemeliharaan dokumentasi.
- **GASSP.** Generally Accepted System Security Principles (GASSP) adalah produk dari Dewan Riset Nasional Amerika Serikat. Penekanan adalah pada alasan penentuan kebijakan keamanan.
- **ISF Standard of Good Practice.** The Information Security Forum Standard mengambil pendekatan baseline, dengan memberikan perhatian yang cukup banyak pada perilaku pengguna yang diharapkan untuk kesuksesan program tersebut. Edisi 2005 berisi topik-topik seperti pesan instan yang aman, keamanan server WEB dan perlindungan virus.

Peraturan Pemerintah

- Both United States and United Kingdom telah menentukan standar dan menetapkan peraturan yang ditujukan untuk menanggapi masalah pentingnya keamanan informasi yang makin meningkat.
- U.S. Government Computer Security Standards.
  - Seperangkat standar keamanan yang harus dipenuhi oleh organisasi-oraganisasi yang berpartisipasi.
  - Tersedianya program perangkat lunak yang menilai sistem para pengguna dan membantu mereka dalam mengonfigurasi sistem mereka untuk memenuhi standar.
  - UU Antiterorisme, kejahatan dan keamanan Inggris (ATCSA, 2001)

Standar Industri

- **Center for Internet Security (CIS)** organisasi nirlaba yang didedikasikan untuk membantu para pengguna komputer guna membuat sistem mereka lebih aman.
  - **CIS Benchmarks** membantu para pengguna untuk mengamankan sistem informasi mereka dengan cara menerapkan pengendalian khusus teknologi.
  - **CIS Scoring Tools** memberi kemampuan bagi pengguna untuk menghitung tingkat keamanan, membandingkannya dengan tolok ukur, dan menyiapkan laporan yang mengarahkan pengguna dan administrator sistem untuk mengamankan sistem.

Sertifikasi Profesional

- Mulai tahun 1960-an, profesi TI mulai menawarkan program sertifikasi cakupan dari program-program ini:
  - *Information Systems Audit and Control Association* (*ISACA*)
  - *International Information System Security Certification Consortium* (*ISC*)
  - *SANS* (*SysAdmin, Audit, Network, Security*) *Institute*

Manajemen Kelangsungan Bisnis

- **Business continuity management** (**BCM**) aktivitas yang ditujukan untuk menentukan operasional setelah terjadi gangguan sistem informasi.
- Perencanaan bencana (**disaster planning)**, namun istilah yang lebih positif adalah perencanaan kontijensi (**ontingency planning)**.
- **Contingency plan** merupakan dokumentasi tertulis formal yang menyebutkan secara detail tindakan-tindakan yang harus dilakukan jika terjadi gangguan, atau ancaman gangguan, pada operasi komputasi perusahaan.

Sub-rencana Kontijensi

- **Emergency plan** (rencana darurat) menyebutkan cara-cara yang akan menjaga keamanan karyawan jika bencana terjadi.
  - Mencakup sistem alarm, prosedur evakuasi dan sistem pemadaman api.
- **Backup plan** (rencana cadangan) mengatur agar fasilitas yang biasa hancur atau rusak tidak dapat digunakan. Pengaturan ini merupakan bagian dari rencana cadangan. Cadangan dapat diperoleh melalui kombinasi redundansi, keberagaman dan mobilitas.
- **Vital records** (catatan penting) adalah dokumen kertas, mikrofon dan media penyimpanan optis dan magnetis yang penting untuk meneruskan bisnis perusahaan tersebut.
- **Vital records plan** (rencana catatan penting) menentukan cara bagaimana catatan penting tersebut harus dilindungi. Selain menjaga catatan tersebut di situs komputer, salinan cadangan harus disimpan di lokasi yang terpencil.