LECTURE NOTES

Managing IT for the Enterprise

LEARNING OUTCOMES

1. Menjelaskan teknologi informasi untuk keunggulan kompetitif
2. Menjelaskan aplikasi sistem untuk penyelesaian maslah

OUTLINE MATERI:

1. *Managing IT for the Enterprise*
- *Business and IT*
- *Managing information technology*
- *Business IT planning*
- *Managing the IT function*
- *Organizing IT*
- *Outsourcing and offshoring IT and IS*
- *Failures in IT management*

2. *Managing Global IT The*
- *international dimension*
- *Global IT management*
- *Cultural, political, and geoeconomic challenges*
- *Global business IT strategies*
- *Global business IT applications*
- *Global IT platforms*
- *Global data access issues*
- *Global system development*

3. *Security , Ethical, and Societal Challenges of IT*
- *Introduction*
- *Reinventing security*
- *Computer crime*
- *Other issues*

4. *Security Management of Information Technology*
- *Introduction*
- *Tools of security management*
- *Inter-networked security defences*
- *Viral defences*
- *Other security measures*
- *System control and audits*

ISI MATERI

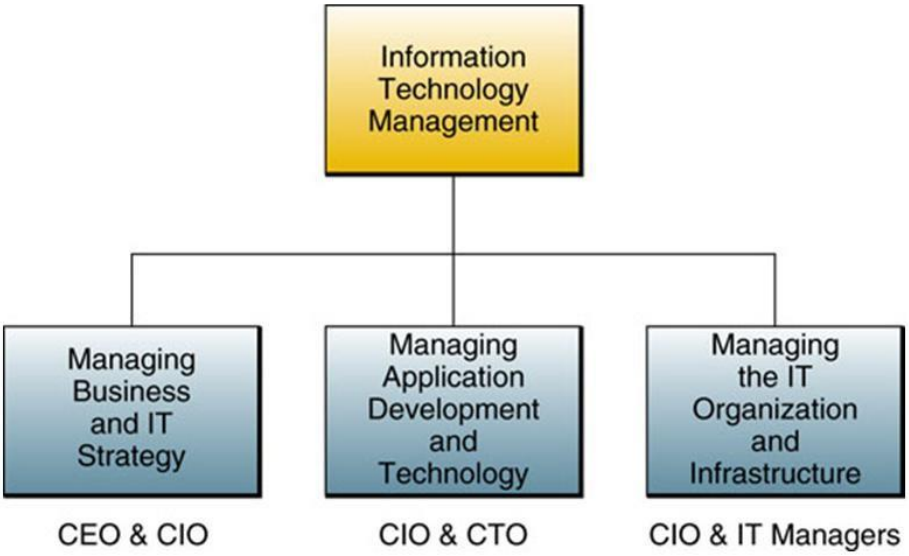
Managing IT for the Enterprise Business and IT

Kepentingan strategis dan operasional teknologi informasi dalam bisnis sudah tidak lagi dipertanyakan. Sepanjang abad ke-21, banyak perusahaan diseluruh dunia berkeinginan berubah

ke kelompok besar bisnis global melalui investasi global dalam e-business, e-commerce, dan inisiatif dari teknologi informasi lainnya. Jadi sudah menjadi kebutuhan bagi para manajer dan profesional bisnis untuk memahami dan mengerti bagaimana mengelola fungsi-fungsi utama dari bisnis. Seorang manajer atau profesional bisnis mengelola teknologi informasi akan menjadi salah satu tugas dan tanggungjawabnya.

Managing information technology

Teknologi informasi merupakan komponen utama dari keberhasilan bisnis suatu perusahaan saat ini, tetapi teknologi informasi juga merupakan sumberdaya penting yang perlu dikelola dengan baik. Selanjutnya perlu diketahui juga contoh-contoh nyata, kapan pengelolaan teknologi informasi berperan utama dalam keberhasilan atau ikut berkontribusi dalam kegagalan mendukung strategi perusahaan. Oleh karenanya pengelolaan sistem informasi dan teknologi yang mendukung proses-proses bisnis maju dalam perusahaan saat ini, merupakan tantangan utama bagi para manajer dan profesional bisnis. Gambar 10.1 berikut memperlihatkan salah satu bagaimana teknologi informasi dari perusahaan berskala besar dikelola dengan baik.



Gambar 10.1 *The major components of information technology mnagement*

Business IT planning

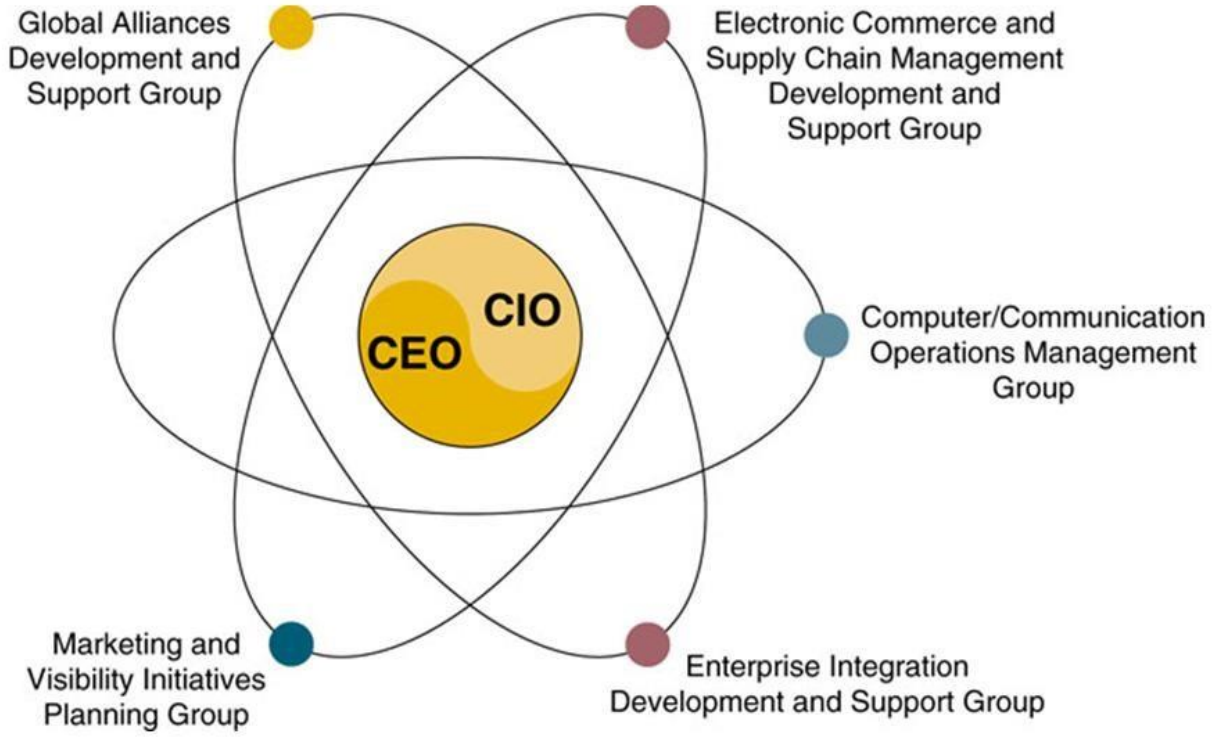
Proses perencanaan bisnis/TI difokuskan pada bagaimana memperoleh pendekatanpendekatan inovatif untuk memenuhi nilai yang diinginkan para pelanggan dan nilai bisnis tujuan perusahaan. Proses perencanaan akan mengarahkan pengembangan strategi dan modelmodel bisnis pada aplikasi-aplikasi bisnis yang baru, proses-proses bisnis yang baru, serta produk dan jasa yang baru. Selanjutnya perusahaan akan mengembangkan strategi TI dan arsitekturnya yang mendukung pembangunan dan implementasi aplikasi-aplikasi bisnis yang baru

direncanakan.Proses perencananaan bisnis TI mempunyai tiga komponen utama, yaitu: *strategy development* (pengembangan strategi-strategi bisnis yang mendukung visi bisnis perusahaan), *resources management* (pengembangan rencana-rencana strategis untuk mengelola sumberdaya TI perusahaan, termasuk: perngkat keras, perangkat lunak, jaringan, data, dan personel), dan *technology development (*membuat pilihan-pilihan strategi TI yang dituangkan dalam arsitektur teknologi informasi untuk mendukung inisiatif bisnis/TI*).*

Arsitektur teknologi informasi yang dibangun dalam proses perencanaan strategi bisnis/TI merupakan konsep rancanga, atau blueprint, yang mencakup empat komponen yaitu: platform teknologi (technology platform), sumberdaya data (data resources), arsitektur aplikasi (applications architecture), dan organisasi TI (IT organization).

Managing the IT function Organizing IT

Pengelolaan fungsi TI dimulai dengan bagaimana organisasi TI. Pada tahun-tahun awal komputasi, pengembangan komputer berskala besar (mainframe), jaringan komunikasi data, dan terminal-terminal interface, menyebabkan sentralisasi (centralization) dari perangkat keras dan perangkat lunak komputer, database, dan spesialis-spesialis informasi pada tingkat perusahaan. Era berikutnya, pengembangan mini komputerdan micro komputer mempercepat tren *downsizing*, yang memperlihatkan kembalinya pendekatan desentralisasi (*decentralization*) oleh banyak perusahaan. Akhir-akhir ini, tren focus pada membangun kontrol yang lebih terpusat atas pengelolaan sumber daya perusahaan TI, disamping masih melayani kebutuhan strategis unit bisnis, terutama e-bisnis mereka dan inisiatif e-commerce. Tren ini mengakibatkan terjadi pengembangan struktur yang campuran (hibrida) dengan kombinasi dua komponen yaitu komponen sentralisasi dan komponen desentralisasi. Gambar 10.2 berikut memperlihatkan komponen-komponen fungsi TI dalam organisasi modern.



Gambar 10.2 *The IT functions in modern organization*

Beberapa hal yang perlu diperhatikan dalam pengelolaan berbagai fungsi dan kegiatan dalam sistem informasi adalah: pengelolaan pengembangan aplikasi, pengembangan operasi sistem informasi, perencanaan staf TI, eksekutif TI, manajemen teknologi, dan pengelolaan layanan kepada pengguna.

Outsourcing and offshoring IT and IS

Outsourcing. *Outsourcing* adalah pembelian barang atau jasa yang semula disediakan secara internal menjadi diadakan oleh patner atau pihak ketiga. Fungsi TI yang biasanya dioutsourcing- kan adalah pengembangan perangkat lunak aplikasi. Proses ini termasuk penangangan kontrak atau sub-kontrak dengan pihak luar organisasi untuk pengembangan baik seluruh atau sebagian produk perangkat lunak atau proyek TI, pembelian paket perangkat lunak atau produk perangkat lunak aplikasi, atau kegiatan-kegiatan yang termasuk dalam siklus hidup pengembangan sistem. Gamba2 10.3 berikut memperlihatkan sepuluh teratas dari masing-masing isu outsourcing, yaitu pengembangan yang biasanya dilakukan oursoucing, alasan-alasan mengapa perlu outsorcing, factor-faktor yang keberhasilan outsourcing, dan pemilihan vendor pelaksana outsourcing.

Top 10 Reasons Companies Outsource	Top 10 Factors in Vendor Selection
1. Reduce and control operating costs	1. Commitment to quality
2. Improve company focus	2. Price
3. Gain access to world-class capabilities	3. References/reputation
4. Free internal resources for other purposes	4. Flexible contract terms
5. Necessary resources are not available internally	5. Scope of resources
6. Accelerate reengineering benefits	6. Additional value-added capability
7. Function is difficult to manage internally or is out of control	7. Cultural match
8. Make capital funds available	8. Existing relationship
9. Share risks	9. Location
10. Cash infusion	10. Other
Top 10 Factors for Successful Outsourcing	**Top 10 IT Areas Being Outsourced**
1. Understand company goals and objectives	1. Maintenance and repair
2. A strategic vision and plan	2. Training
3. Select the right vendor	3. Applications development
4. Ongoing management of the relationships	4. Consulting and reengineering
5. A properly structured contract	5. Mainframe data centers
6. Open communication with affected individuals/groups	6. Client/server services and administration
7. Senior executive support and involvement	7. Network administration
8. Careful attention to personnel issues	8. Desktop services
9. Near-term financial justification	9. End-user support
10. Use of outside expertise	10. Total IT outsourcing

Gambar 10.3 *Outsourcing's top 10 Issues*

Offshoring. Istilah ini sering membingungkan terutama dengan pengertian outsourcing, tetapi lambat laun offshoring juga menjadi bagian strategi dari bisnis/TI. Offshoring adalah usaha relokasi proses-proses bisnis (termasuk produksi/manufaktur) ketempat yang lebih murah, umumnya keluar negeri. Jadi konteks offshoring dapat berkaitan produksi dan dapat pula berkaitan dengan jasa. Perkembangan layanan offshoring dalam teknologi informasi terjadi karena tersedianya infrastruktur telekomunikasi dengan jumlah besar, dapat dipercaya, dan terjangkau sejak tahun 1990-an.

Failures in IT management

Mengelola teknologi informasi bukan maslah yang mudah. Fungsi-fungsi dari sistem informasi daalam organisasi kadang-kadang mempunyai masalah-masalah kinerja sistem. Manfaat yang dijanjikan pada saat pengembangan sistem informasi ternyata tidak menjadi kenyataan. Sudi atau penelitian dari berbagai pihak termasuk perguruan tinggi menyimpulkan bahwa banyak perusahaan yang gagal atau tidak berhasil dalam mengelola penggunaan teknologi informasi yang dimilikinya. Dua contoh kegagalan yang sering terjadi adalah:

1. Teknologi informasi tidak digunkan secara efektif oleh perusahaan yang menggunakan TI khusunya untuk komputerisasi proses-proses binis tradisional, apalagi dengan pengembangan inovasi e-business yang mencakup pelanggan, pemasok, bisnis dengan patner kerja, e-commerce, dukungan keputusan berbasis web.

2. Teknologi informasi tidak digunkan secara efisien oleh sistem informasi yang menyediakan respon lambat dan sering tidak beroperasi (down), atau oleh profesional bisnis dan konsultan yang tidak dapat mengelola proyek-proyek pengembangan aplikasi.

Apa solusi dari kegagalan ini, ternyata tidak mudah untuk ditemukan. Berdasarkan pengalaman dari beberapa perusahaan yang sukses, menyatakan dua aspek yang perlu diperhatikan adalah: *management involvement* dan *IT governance*.

Management involvement. Partisipasi atau keikutsertaan manajemen dan pengguna akhir merupakan kunci keberhasilan untuk meningkatkan kinerja dari sistem informasi. Gambar 10.4 berikut peran keikutsertaan manajemen dan akibat yang dihadapi bila tidak terlibat dalam pengembangan dan implementasi sistem.

IT Decision	Senior Management's Role	Consequences of Abdicating the Decision
• How much should we spend on IT?	Define the strategic role that IT will play in the company, and then determine the level of funding needed to achieve that objective.	The company fails to develop an IT platform that furthers its strategy, despite high IT spending.
• Which business processes should receive our IT dollars?	Make clear decisions about which IT initiatives will and will not be funded.	A lack of focus overwhelms the IT unit, which tries to deliver many projects that may have little companywide value or can't be implemented well simultaneously.
• Which IT capabilities need to be companywide?	Decide which IT capabilities should be provided centrally and which should be developed by individual businesses.	Excessive technical and process standardization limit the flexibility of business units, or frequent exceptions to the standards increase costs and limit business synergies.
• How good do our IT services really need to be?	Decide which features—for example, enhanced reliability or response time—are needed on the basis of their costs and benefits.	The company may pay for service options that, given its priorities, aren't worth their costs.
• What security and privacy risks will we accept?	Lead the decision making on the trade-offs between security and privacy on one hand and convenience on the other.	An overemphasis on security and privacy may inconvenience customers, employees, and suppliers; an underemphasis may make data vulnerable.
• Whom do we blame if an IT initiative fails?	Assign a business executive to be accountable for every IT project; monitor business metrics.	The business value of systems is never realized.

Gambar 10.4 *Involvement of Senior Management in Critical Business/IT Decisions*

IT *Governance*. Tata kelola teknologi informasi atau information technology governance (ITG) merupakan bagian dari tata kelola perusahaan yang difokuskan pada teknologi informasi, sistem informasi, kinerjanya, pengguanaanya, dan resiko yang diakibatkannya. Fokus dari ITG adalah keputusan menetapkan masukan-masukan dan aturan-aturan, diikuti dengan kerangka tanggungjawab yang melekat berkaitan dengan tata kelola sistem.

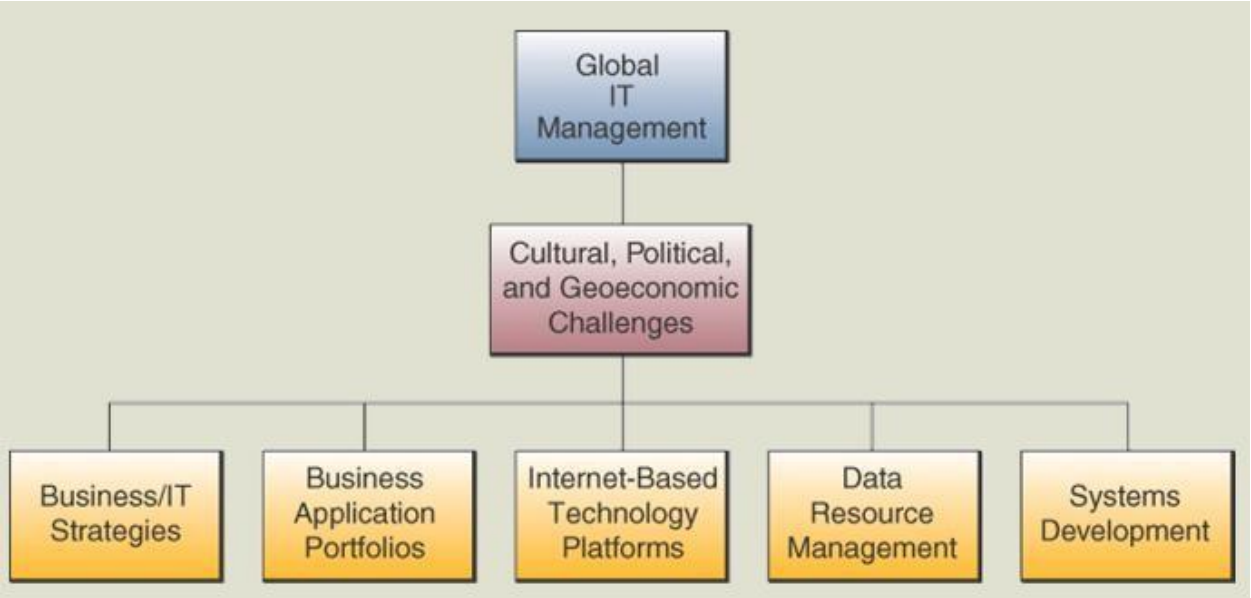
Managing Global IT The international dimension

Dimensi-dimensi internasional telah menjadi bagian yang sangat penting dalam pengelolaan bisnis atau perusahaan besar dalam jaringan interkoneksi ekonomi dan pasar global saat ini. Para manajer perusahaan besar atau pemilik perusahaan kecil tetap akan terpengaruh oleh

pengembangan-pengembangan bisnis internasional karena tetap akan berhubungan dengan pebisnis, produk dan jasa, yang berasal dari negaranya masing-masing.

Global IT management

Gambar 10.5 berikut menggambarkan dimensi-dimesi utama dari pekerjaan mengelola teknologi informasi global yang saat ini harus dilakukan. Pengembangan bisnis yang sesuai dengan strategi-startegi TI dalam menghadapi pasar global akan manjadi langkah pertama dalam majajemen teknologi informasi global (*global information technology management)*.



Gambar 10.5 The Global IT Management

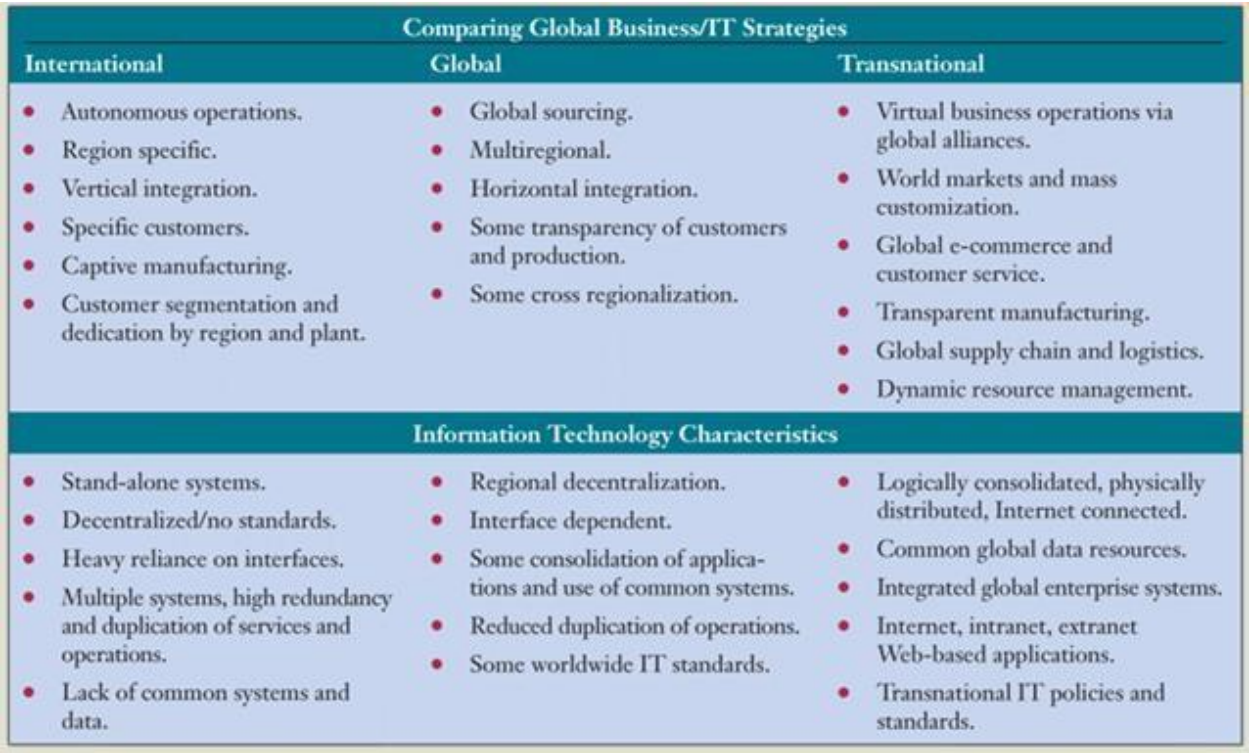
Cultural, political, and geoeconomic challenges

"Business as usual" tidak cukup baik dalam operasi-operasi era bisnis global. Hal yang sama juga benar untuk manajemen teknologi e-business global. Banyak realias yang berkaitan dengan budaya, politik, geografis, dan ekonomi yang harus dihadapi agar bisnis berhasil dipasar global. Manajemen teknologi informasi global harus fokus pada pengembangan strategi-strategi TI dalam bisnis global dan pengelolaan aplikasi e-business global secara nyata, yaitu teknologi internet, plafform, database, dan proyek-proyek pengembangan sistem.

Global business IT strategies

Bisnis bergerak jauh dari strategi-strategi internasional yang didalamnya terdapat anak perusahaan asing yang otonom tetapi proses-proses baru, produk, ide-ide, merke tergantung pada perwakilan pusat atau dari strategi-strategi global, dan disitu operasi-operasi perusahaan dunia

dikelola oleh perusahaan perwakilan pusat. Gambar 10.6 berikut memperlihatkan operasi perusahaan internasional bergerak kearah strategi multinasisonal.

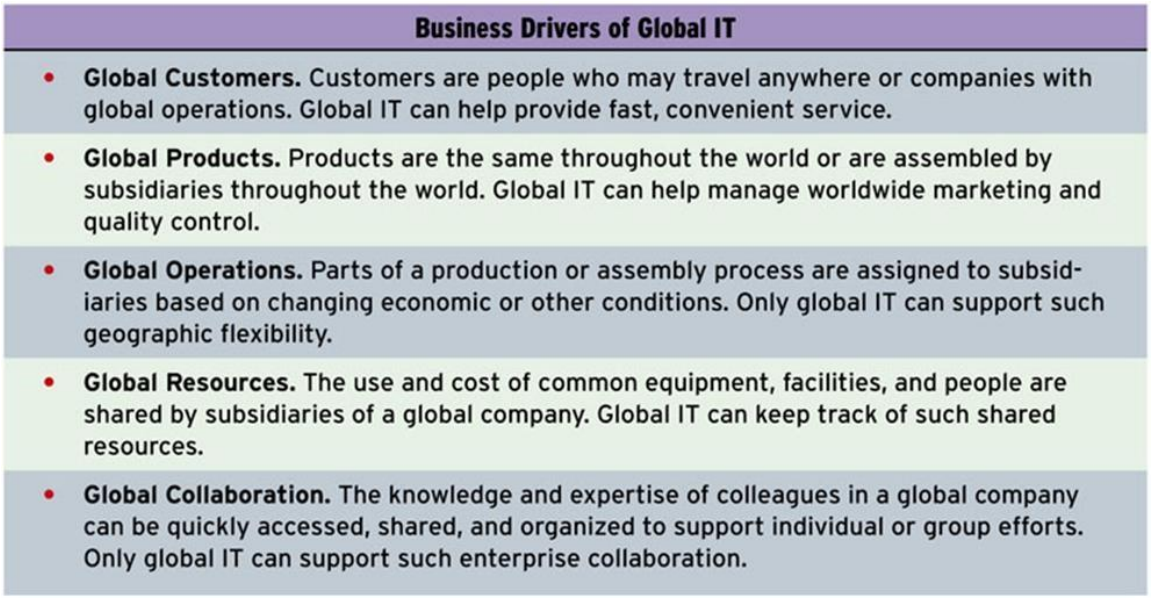


Comparing Global Business/IT Strategies		
International	**Global**	**Transnational**
• Autonomous operations. • Region specific. • Vertical integration. • Specific customers. • Captive manufacturing. • Customer segmentation and dedication by region and plant.	• Global sourcing. • Multiregional. • Horizontal integration. • Some transparency of customers and production. • Some cross regionalization.	• Virtual business operations via global alliances. • World markets and mass customization. • Global e-commerce and customer service. • Transparent manufacturing. • Global supply chain and logistics. • Dynamic resource management.
Information Technology Characteristics		
• Stand-alone systems. • Decentralized/no standards. • Heavy reliance on interfaces. • Multiple systems, high redundancy and duplication of services and operations. • Lack of common systems and data.	• Regional decentralization. • Interface dependent. • Some consolidation of applications and use of common systems. • Reduced duplication of operations. • Some worldwide IT standards.	• Logically consolidated, physically distributed, Internet connected. • Common global data resources. • Integrated global enterprise systems. • Internet, intranet, extranet Web-based applications. • Transnational IT policies and standards.

Gambar 10.6 *Transnational business IT strategies*

Global business IT applications

Aplikasi-aplikasi teknologi informasi dikembangkan oleh perusahaan-perusahaan global berdasarkan pada strategi bisnis/Ti global mereka dan juga keakhlian dan pengalaman yang dimilikinya. Tentu aplikasi-aplikasi itu akan bergantung pada berbagai macam pendorong bisnis global (*global business drivers*), yaitu persyaratan-persyaratan bisnis yang diturunkan dari industri utama dan daya dorong kompetitif dan lingkungan usaha. Gambar 10.7 berikut menjelaskan ringkasan dari beberapa persyaratan-persyaratan bisnis yang membuat TI global menjadi kebutuhan kompetitif.



Business Drivers of Global IT
• **Global Customers.** Customers are people who may travel anywhere or companies with global operations. Global IT can help provide fast, convenient service.
• **Global Products.** Products are the same throughout the world or are assembled by subsidiaries throughout the world. Global IT can help manage worldwide marketing and quality control.
• **Global Operations.** Parts of a production or assembly process are assigned to subsidiaries based on changing economic or other conditions. Only global IT can support such geographic flexibility.
• **Global Resources.** The use and cost of common equipment, facilities, and people are shared by subsidiaries of a global company. Global IT can keep track of such shared resources.
• **Global Collaboration.** The knowledge and expertise of colleagues in a global company can be quickly accessed, shared, and organized to support individual or group efforts. Only global IT can support such enterprise collaboration.

Gambar 10.7 *The Business Drivers of Global IT* ***Global IT platforms***

International Data Communications Issues
Network Management Issues
• Improving the operational efficiency of networks.
• Dealing with different networks.
• Controlling data communication security.
Regulatory Issues
• Dealing with transborder data flow restrictions.
• Managing international telecommunication regulations.
• Handling international politics.
Technology Issues
• Managing network infrastructure across countries.
• Managing international integration of technologies.
Country-Oriented Issues
• Reconciling national differences.
• Dealing with international tariff structures.

Gambar 10.8 *International Data Communication Issues*

Manajemen platform-platform teknologi merupakan dimensi penting lain dari manajemen TI global, seperti pengelolaan perangkat keras, perangkat lunak, sumberdaya data, jaringan, serta fasilitas komputasi lainnya yang mendukung operasi-operasi bsinis global. Manajemen platform TI global tidak hanya sulit dan kompleks secara teknik, tetapi juga mempunyai implikasi politik

dan budaya. Misalnya, banyak terjadi pemilihan perangkat keras disuatu negara menjadi sulit karena harus memperhatikan factor-faktor pembatasan impor, pajak, dukungan suku cadang, ataupun perlunya persetujuan dari pemerintah. Dalam pemilihan perangkat lunak sering terjadi masalah kompatibelitas, lisensi, maupun tidak tersediannya distributor local. Gambar 10.8 diatas memperilhatkan isu-isu teknologi yang menekankan pentingnya manajemen telekomunikasi global. Internet merupakan salah satu platform TI global, dan saat ini internet dengan world wide web menjadi komponen penting dalam bisnis dan perdagangan internasional. Dengan menghubungkan bisnis kedalam jaringan internet global, maka perusahaan akan meningkatkan peluang dan target lokasi pasar, memotong biaya komunikasi dan distribusi, dan meningkatkan margin keuntungan. Gambar 10.9 berikut memperlihatkan statistik jumlah pengguna internet diseluruh dunia. Perhatikan bahwa dengan jumlah penduduk dunia pada tahun 2005, jumlah yang menggunakan internet sudah mencapai 888.681.131 pengguna, dengan pertumbuhan yang diatas 100% maka dapat diperkirakan jumlah pengguna pada tahun 2013 sudah beberapa kali lipat.

World Internet Usage and Population Statistics						
World Regions	Population (2005 Est.)	Population % of World	Internet Usage, Latest Data	Usage Growth 2000–2005	Penetration (% Population)	World Users %
Africa	900,465,411	14.0 %	13,468,600	198.3%	1.5%	1.5%
Asia	3,612,363,165	56.3	302,257,003	164.4	8.4	34.0
Europe	730,991,138	11.4	259,653,144	151.9	35.5	29.2
Middle East	259,499,772	4.0	19,370,700	266.5	7.5	2.2
North America	328,387,059	5.1	221,437,647	104.9	67.4	24.9
Latin America/Caribbean	546,917,192	8.5	56,224,957	211.2	10.3	6.3
Oceania / Australia	33,443,448	0.5	16,269,080	113.5	48.6	1.8
WORLD TOTAL	6,412,067,185	100.0	888,681,131	146.2	13.9	100.0

Gambar 10.9 *Internet users by World Region*

Global data access issues

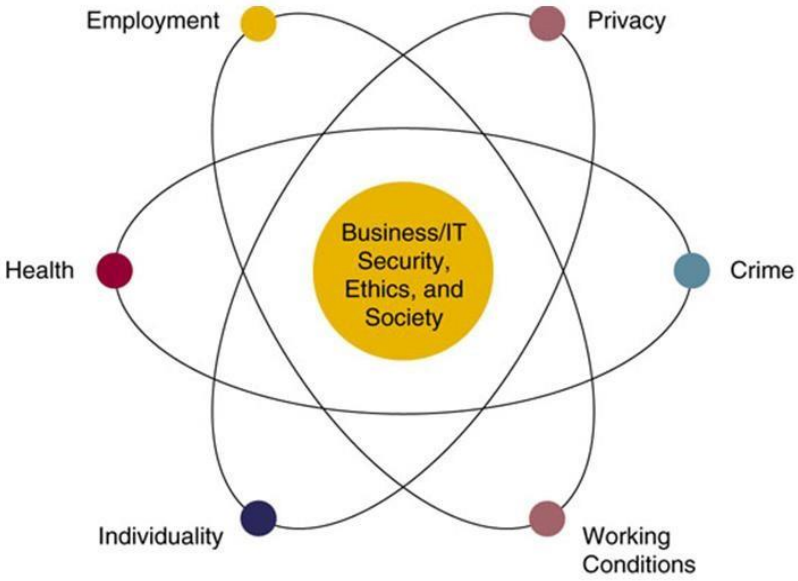
Dalam beberapa tahun ini, isu-isu akses ke data global telah menjadi pokok kontraveri politik dan hambatan teknologi dalam operasi-operasi bisnis global menjadi lebih nyata dengan perkembangan internet dan e-commerce. Contoh yang sudah banyak diketahui adalah isu *transborder data flows* (TDF), yaitu aliran data bisnis lintas batas-batas internasional melalui

jaringan-jaringan telekomunikasi dari sistem-sistem informasi global. Banyak negara menganggapnya sebagai suatu pelanggaran karena data mengalir tanpa melalui bea masuk dan regulasi ekpor dan impor barang dan jasa. Dalam banyak kasus, isu aliran data bisnis yang secara politik sensitif adalah keluarnya data keluar negeri, khususnya data personal yang berada dalam aplikasi e-commerce dan aplikasi sumberdaya manusia.

Global system development

Coba bayangkan bagaimana pengembangan aplikasi-aplikasi yang efektif, efisien dan responsif untuk kebutuhan bisnis dan pengguna-pengguna dalam negeri, kemudian gandakan dengan banyak jumlah negara dan budayanya yang mungkin menggunakan sistem e-business. Itulah tantangan dari pengelolaan pengembangan sistem global. Disana pasti ada konflik kepentingan local dangan persyaratan-persyaratan pada sistem global, seperti cocok tidaknya fitur yang dikembangkan, bahasa, dan rancangan dengan standard baku. Isu lain yang muncul adalah gangguan diakibatkan oleh kegiatan-kegiatan implementasi dan pemeliharaan sistem. Misalnya, dalam kaitannya dengan waktu, siang hari disuatu negara bersamaan dengan dengan malam hari dinegara lain. Beberapa strategi menghadapi pengembangan sistem global adalah sebagai berikut: Pertama, tranformasikan aplikasi yang saat ini digunakan dikantor (local) ke aplikasi-aplikasi global. Kedua, siapkan tim pengembangan multinasional dengan anggota dari masing-masing cabang atau negara untuk menjamin rancangan sistem cocok dengan kebutuhan lokal, dan perusahaan di kantor perwakilan. ***Security , Ethical, and Societal Challenges of* IT**

Tidak perlu dipertanyakan lagi bahwa penggunaan teknologi informasi dalam bisnis akan membawa tantangan-tantangan keamanan, etika yang harus dimiliki, dan pengaruh sosial lainnya. Penggunaan teknologi informasi dalam bisnis mempunyai dampak yang besar pada masyarakat baik dampak positif dan negatif yang timbul. Dampak negatif yang ditimbulkan akan berkaitan dengan penggunaan yang salah dan etika dalam banyak isu seperti : kejahatan, kerahasiaan pribadi, peluang kerja, ksehatan dan kondisi kerja. Gambar 10.10 berikut memperlihatkan aspek-aspek penting dari sisi keamanan, etika dan dimensi-dimensi penggunaan teknologi informasi dalam bisnis. Perlu diingat bahwa teknologi informasi dapat digunakan baik untuk hal-hal yang menguntungkan masyarakat maupun yang merugikan masyarakat.



Gambar 10.10 *Security, Ethical, and Societal Aspects of IT Use*

Business ethics. Etika bisnis berkaitan dengan sejumlah pertanyaan yang harus dihadapi dan direspon sebagai bagian dari pengambilan keputusan bisnis sehari-hari. Gambar 10.11 berikut memperlihatkan ringkasan dari katagori isu-isu etika dalam bisnis.

Equity	Rights	Honesty	Exercise of Corporate Power
Executive salaries	Corporate due process	Employee conflicts of interest	Product safety
Comparable worth	Employee health screening	**Security of company information**	Environmental issues
Product pricing	**Customer privacy**	Inappropriate gifts	Disinvestment
Intellectual property rights	**Employee privacy**	Advertising content	Corporate contributions
Noncompetitive agreements	Sexual harassment	Government contract issues	Social issues raised by religious organizations
	Affirmative action	Financial and cash management procedures	Plant/facility closures and downsizing
	Equal employment opportunity	Questionable business practices in foreign countries	Political action committees
	Shareholder interests		**Workplace safety**
	Employment at will		
	Whistle-blowing		

Gambar 10.11 Catagories of Ethical Business Issues

Perhatikan bahwa penekanan pada beberapa isu tentang hak cipta intelektual (intellectual property right), privasi pelanggan (customer privacy), privasi karyawan (employee privacy), keamanan informasi perusahaan (security of company information), keamanan tempat bekerja (workplace safety), karena merupkan area yang banyak terjadi kontraversi dalam penggunaan teknologi informasi. Bagaimana manajer mengambil keputusan yang bersifat etika, bila harus menghadapi masalah yang dijelaskan dalam Gambar 10.11, perlu memperhatikan prinsip atau teori yang ada dalam tugas dan tanggung jawab perusahaan.

Ethical the use of technology

Selain etika yang bersifat umum, dalam penggunaan teknologi informasi juga perlu dianut prinsip-prinsip: *proportionality, inform consent., justice* dan *minimize risk*, seperti terlihat pada Gambar 10.12 berikut. Prinsip ini dapat dipakai sebagai etika dasar yang harus dipenuhi oleh perusahaan untuk menjamin agar etika dijalankan dalam implementasi teknologi informasi dan dalam sistem informasi bisnis.

Gambar 10.12 The Principles of Technology Ethics

Computer crime

Oleh AITP (Association of Information Technology Professionals) yang termasuk dalam kejahatan komputer (computer crime) adalah: *1). Unauthorized use, access, modification, or destruction of hardware, software, data, or network resources; 2). The unauthorized release of information; 3). The unauthorized copying of software; 4). Denying an end user access to his/her own hardware, software, data, or network resources;* dan *5). Using or conspiring to use computer or network resources illegally to obtain information or tangible property.*

Dalam dunia komputer hacking adalah penggunaan komputer yang obesif atau secara tidak sah masuk (unauthorized access) kedalam jaringan sistem komputer. Hacker dapat sebagai karyawan perusahaan atau pihak-pihak diluar perusahaan yang menggunakan internet atau jaringan lainnya utnuk mencuri atau merusak data atau program komputer. Para hacker dapat mencuri atau merusak program komputer dengan berbagai macam cara berikut.

Denial of service	By hammering a website's equipment with too many request for information, attackers can effectively clog the system.
Clogging the system	Slowing performance, or crashing the site

Scans	Widespread probes of the Internet to determine types of computers, services, and connections Looking for weaknesses
Sniffer	Programs that search individual packets of data as they pass through the Internet Capturing passwords or entire contents
Spoofing	Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers
Trojan Horse	A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software
Back Doors	A hidden point of entry to be used in case the original entry point is detected or blocked
Malicious Applets	Tiny Java programs that misuse your computer's resources, modify files on the hard disk, send fake email, or steal passwords
War Dialing	Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection
Logic Bombs	An instruction in a computer program that triggers a malicious act
Buffer Overflow	Crashing or gaining control of a computer by sending too much data to buffer memory
Password Crackers	Software that can guess passwords
Social Engineering	Gaining access to computer systems by talking unsuspecting company employees out of valuable information, such as passwords
Dumpster Diving	Sifting through a company's garbage to find information to help break into their computers

Adanya perbedaan tujuan, komunitas hacker membedakan antara "hacking" dan "cracking". Cracker yang disebut juga sebagai "black hacker" atau "darkside hacker", adalah hacker yang jahat atau yang berbuat criminal.

Perbuatan-perbuatan lainnya yang termasuk dalam kejahatan komputer adalah: Cyber theft (pencurian dalam dunia maya), Cyberterrorism (terror melalui dunia maya), Cyber-warfare (perang dalam dunia maya), Unauthorized use at work (penyalahgunaan komputer dalam pekerjaan), Software piracy (pembajakan perangkat lunak), Theft of intellectual property (pembajakan hak

cipta), Computer viruses and worms (memasukkan virus atu worm kedalam program) and Adware and spyware (penggunaan fasilitas diaplikasi internet tanpa ijin).

Other issues

Isu-isu lain yang berkaitan dengan keamanan, etika dan tantangan sosial adalah: isu-isu yang berkaitan dengan pribadi (*privacy issues*), isu yang berkaitan dengan hukum dan undangundang (*the current state of cyber law*), isu-isu yang berkaitan dengan tantang baru (*other challenges*), isu berkaitan dengan kesehatan (*health issues*) dan isu yang berkaitan dengan masalah sosial (*societal solutions*).

Security Management of Information Technology

Dengan pesatnya penggunaan internet, halangan yang akan terjadi dalam e-commerce adalah adalah tranmisi informasi yang ditentukan oleh bandwidth yang digunakan. Ternyata bukan hanya itu, masalah keamanan ternyata menjadi maslah utama dari implementasi aplikasi tersebut. Seperti telah diungkapkan sebelumnya, banyak sekali tantangan-tantangan yang cukup serius dalam keamanan sistem informasi bisnis. Oleh karenanya perlu digali metoda-metoda apa yang dapat digunakan oleh perusahaan untuk digunakan dalam mengelola keamanan sistem. Para manajer dan profesional bisnis seharusnya juga bertanggungjawab atas keamanan, kualitas, dan kinerja dari penggunaan sistem informasi dalam mendukung unit-unit bisnisnya. Perangkat keras, perangkat lunak, database, jaringan harus diamankan dan dibentengi berbagai langkahlangkah keamanan untuk memastikan kualitas dan penggunaan yang menguntungkan.

Tools of security management

Tujuan adari manajemen keamanan adalah untuk akurasi, integritas dan keamanan dari proses-proses dan semua sumberdaya dari sistem informasi. Dengan demikian, manajemen keamanan yang efektif harus dapat meminimumkan kesalahan, penipuan, dan kerugian-kerugian dalam sistem-sistem informasi yang sekarang ini interkoneksi dengan para pelanggannya, pemasoknya, dan stakeholder lainnya. Gambar 10.13 berikut memperlihatkan bahwa manajemen keamanan merupakan tugas yang sangat komplek dan rumit. Para manajer keamanan sistem (*security manager*) harus bisa memperoleh dan mengintegrasikan berbagai macam perangkat keras dan perangkat lunak yang berkaitan dengan keamanan dan metoda-metodanya untuk mengamankan semua sumberdaya sistem informasi perusahaan.

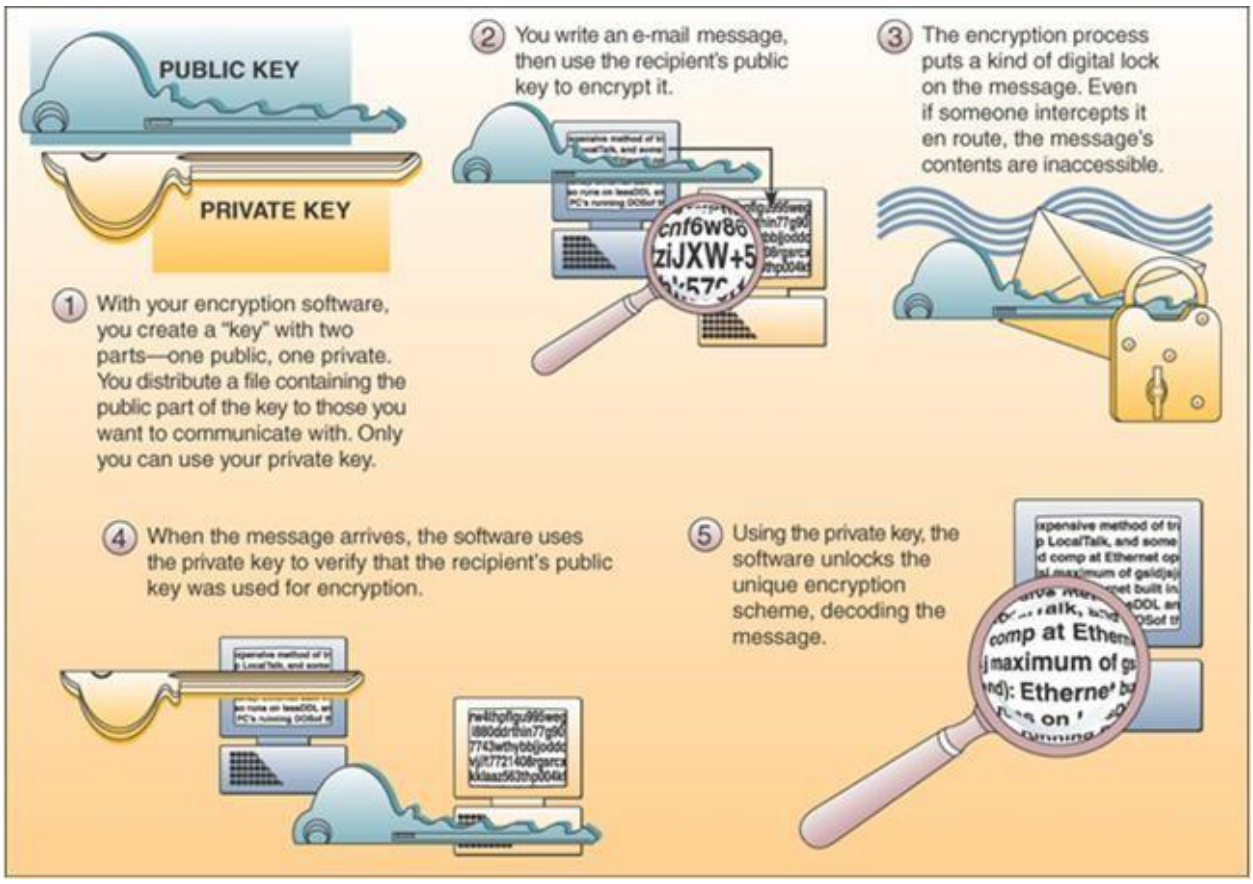
Gambar 10.13 *The Security Management*

Inter-networked security defences

Keamanan dari bisnis perusahaan-perusahaan yang terhubung dalam jaringan global merupakan tantangan utama dari manajemen. Banyak perusahaan yang saat ini masih dalam proses menghubungkan dengan e-commerce, dan merekayas ulang proses bisnis internal mereka menjadi terhubung dengan intranet, e-business dan ekstranet agar terhubung dengan para pelanggan, pemasok, dan patner kerjanya. Hubungan jaringan dan arus informasi bisnis ini perlu dilindungi dari serangan penjahat-penjahat dunia maya atau dari tindakan-tindakan lain yang tidak bertanggungjawab dari internal perusahaan. Perlindungan ini memerlukan berbagai macam peralatan keamanan dan pertahanan serta program manajemen keamanan yang terkoordinasi. Berikut ini beberapa metoda pertahanan dan keamanan yang penting saat ini, yaitu: enkripsi

(*encryption*), anti-intrusi (*firewall*), penolak serangan layanan (*denial of service attacks*) dan pengendalian e-mail (*e-mail monitor*).

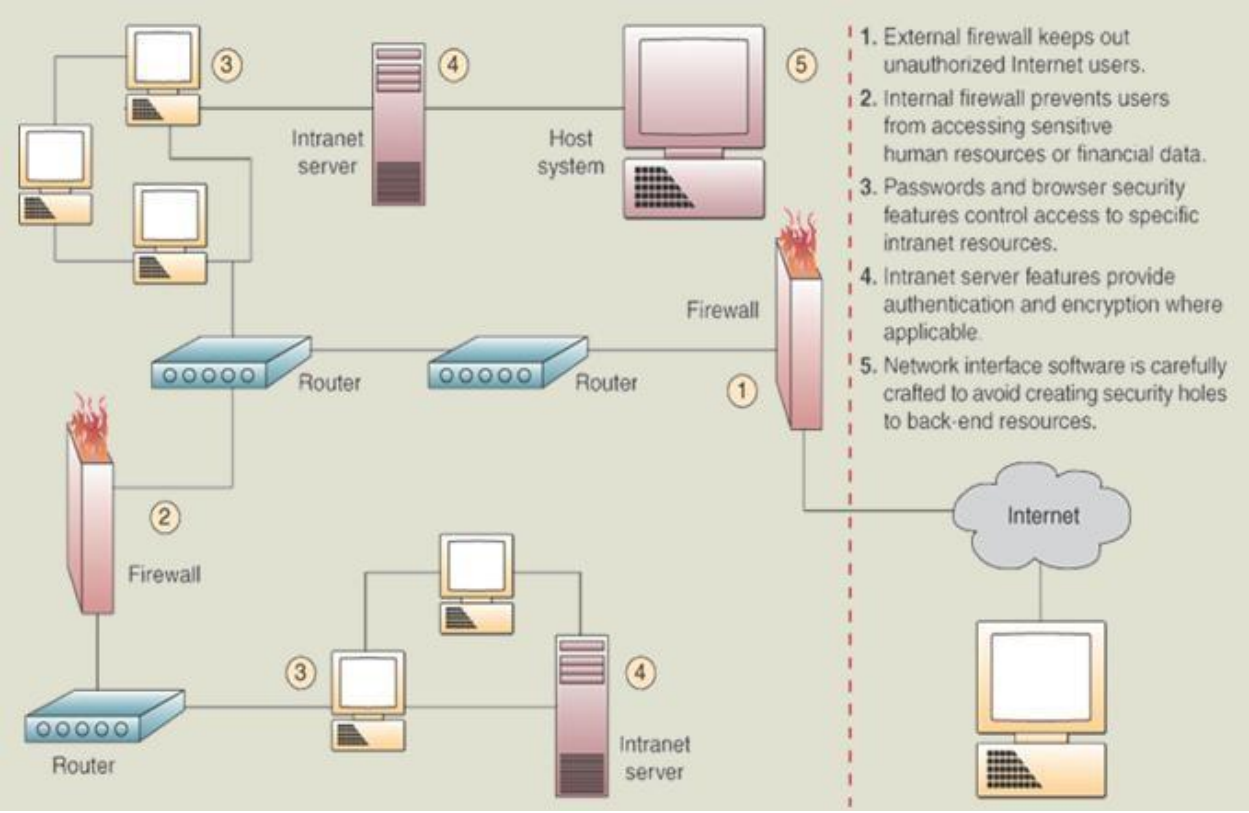
Encryption. Enkripsi data merupakan cara yang sangat penting untuk melindungi data dan sumberdaya jaringan komputer, khususnya internet, intranet dan ekstranet. Password, pesan singkat, file dan data lainnya dapat ditransmisikan dalam bentuk acak dan diatur kembali oleh sistem komputer bagi yang berhak memakai atau menerimanya.Enkripsi dilakukan dengan menggunakan algoritma matematika khusus, atau algoritma kunci, untuk merubah data digital dalam bentuk "code" acak sebelum dikirikan melalui jaringan transmisi, kemudian dilakukan "decode" pada saat data diterima. Gambar 10.14 berikut memperlihatkan bagaimana proses enkripsi bekerja.



Gambar 10.14 *The Encryption Processes*

Firewall. Metoda lain yang juga menting untuk pengawasan dan keamanan dalam internet dan jaringan komunikasi lainnya adalah penggunaan komputer *firewall* dan perngkat lunak. Jaringan firewall dapat suatu communication processor, sering disebut router, atau server khusus

dilengkapi dengan perangkat lunak firewall. Firewall bertugas sebagai benteng penjaga sistem yang melindungi intranet perusahaan atau jaringan lainnya dari intrusi-intrusi atau gangguan-gangguan dari phikal luar dengan menyediakan filter dan pengaman akses ked an dari internet dan dari jaringan lainnya. Gambar 10.15 berikut memperlihatkan firewall intranet dalam jaringan-jaringan perusahaan.



Gambar 10.15 Internet and Intranet Firewalls

***Denial of service attacks*.** Jumlah serangan pada e-commerce dan website perusahaan telah menunjukkan bahwa internet rentan terhadap berbagi serangan dari hacker-hacker kriminal, khususnya serangan dalam bentuk *distributed denial of service* (DDoS). Serangan-serangan melalui internet akan bergantung pada tiga layer jaringan sistem komputer yang bisa menjadi korban, yaitu: 1). situs korban (*the victim's website*), 2). ISP korban (*the victim's internet service provider* (ISP)), dan 3). komputer bantuan yang diaktifkan oleh hacker (*the size of "zombie" or slave computer that the cyber-criminal commandeered*). Berikut ini adalah langkah-langkah bagaimana dapat bertahan secara mandiri dari serangan layanan DDoS.

1. Ditingkat mesin "zombie", tetapkan dan tegakkan kebijakan keamanan sistem. Scan secara teratur untuk mendeteksi dan membersihkan Trojan Horse. Tutuplah port yang tidak digunakan, dan jangan membuka surat dengan extension .exe.

2. Ditingkat ISP. Monitor dan blokir peningkatan lalu lintas, saring alamat IP palsu, dan koordinasikan pengamanan dengan penyedia jaringan.
3. Ditingkat situs web korban. Buatlah server cadangan dan koneksi jaringan cadangan. Batasi koneksi ke server, pasang multiple sistem pendeteksi intrusi dan multiple router untuk mengatasi lalulintas masuk dan mengurangi titik-titik kelemahan.

E-mail monitoring. E-mail juga merupakan tempat yang menjadi sasaran para hacker menyebarkan virus dan menerobos masuk kedalam jaringan komputer. Pengendalian e-mail juga merupakan ajang untuk mencoba menerapkan kebijakan untuk tidak menerima pesan ilegal, personal, dan bentuk-bentuk lain yang bisa merusak pesan.

Viral defences

Banyak perusahaan yang sedang mengembangkan dan membangun pertahanan menghadapi virus yang cepat menyebar dengan pemusatan distribusi dan peremajaan perngkat lunak antivirus sebagai tanggung jawab dari departemen SI. Perusahaan lain melakukan kegiatan outsourcing tanggungjawab perlindungan dari serangan virus pada penyediaan layanan internet atau telekomunikasi atau manajemen keamanan perusahaan.

Other security measures

Secara singkat dapat dipelajari bahwa berbagai alat keamanan digunakan untuk melindungi sistem-sistem bisnis dan jaringan-jaringannya. Hal ini meliputi peralatan perangkat keras dan perangkat lunak, seperti perangkat keras dan lunak komputer, prosedur dan kebijakan pengamanan, password, dan file-file cadangan/duplikat atau file back-up.

Security codes. Sistem password multilevel biasanya digunakan untuk manajemen keamanan (security management). Pertama, pengguna akan log-on kedlam sistem komputer dengan memasukkan kode identifikasi diri atau "user-ID". Kedua, pengguna akan diminta memasukkan password untuk akses kedalam komputer. Ketiga, untuk akses ke file individual, nama file yang unique harus dimasukkan.

Back-up file. File back-up adalah duplikat atau "copy" dari data atau program. File juga bissa di-protek dengan file-file sebelumnya, sehingga bila file rusak masih bisa digantikan dengan file-file sebelumnya. Untuk file utama (master file), back-up dilakukan secara berkala sehingga dikenal dengan *child, parent, grandparent*.

Security monitors. Keamanan dari jaringan dapat dimonitor dengan paket perangkat lunak sistem yang dikenal dengan *system security monitors*. Sistem ini merupakan programprogram yang

memonitor penggunaan sistem komputer dan jaringan dan melindunginya dari penggunaan yang tidak sah, pencurian, dan perusakan sistem.

Biometrik security. Dalam bidang keamanan komputer, biometric security berkembang dengan pesat. Alat ini disediakan oleh komputer untuk mengukur cirri kas fisik yang membedakan setiap individu, termasuk melalui suara, sisik jari, geometri tangan, dinamika tanda tangan, analisis penekanan tombol, retina mata, pengenalan wajah dan analisia genetik.

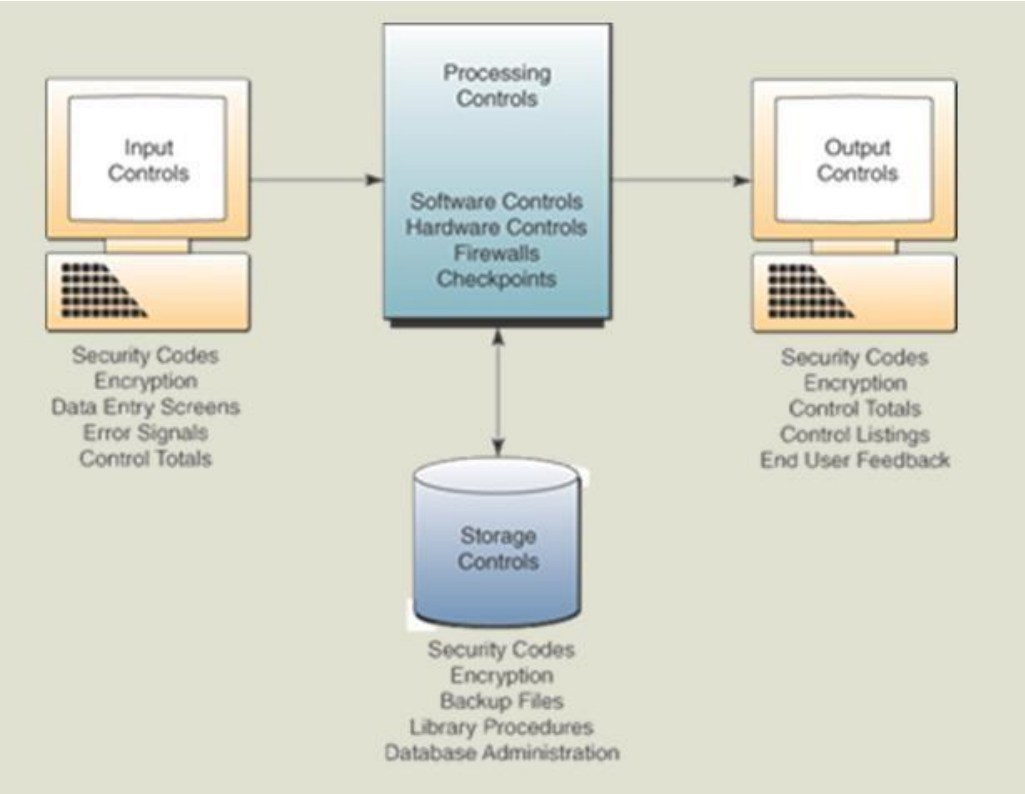
Computer failure control. Sistem komputer gagal karena beberapa alas an, misalnya listrik mati, tidk berfungsinya sirkuit elektronik, ganguan jaringan, kesalahan pemrograman, virus, kesalahan operator, dan juga kalau ada pihak yang merusaknya. Untuk menghindarinya beberapa pendekatan dapat dilakukan, seperti pemeliharaan sistem komputer dan jaringan secara otomatis atau kemampuan pemeliharaan jarak jauh. Kemampuan back-up sistem juga perlu dilakukan dalam program *disaster recovery organizations*. Tidak kalah penting adalah tersedianya tenaga yang terlatih dan menggunakan perangkat lunak manajemen keamanan yang berkinerja baik juga akan mebuat sistem bekerja sesuai dengan harapan.

Fault-tolerants system. Banyak perusahaan ynag menggunakan sistem komputer toleransi kegagalan (*fault tolerant*) yang memiliki banyak processor, periperal dan software yang memberikan kemampuan *fail-over* untuk mendukung berbagai komponen bila terjadi kegagalan. Disaster recovey. Bencana alam dan bencana akibat ulah mausia dapat terjadi. Banyak perusahaan terutama perusahaan ritel, penerbangan, maupun bank tidak berdaya karena kehilangan kekuatan komputasi selama beberapa jam. Alasan ini yang membuat perusahaan menyiapkan prosedur pemulihan dari bencana (*disaster recovery*) dan mengesahkannya dalam *disaster recovery plan*.

System control and audits

Information system control. Dua persyaratan akhir dari manajemen keamanan adalah pengembangan penngendalian sistem informasi dan penyelesaian audit sistem bisnis. Pengendalian sistem informasi (*information system control***)** adalah metoda dan alat yang digunakan untuk memastikan apkah akurasi, validitas, dan kebenaran aktivitas sistem informasi. Pengendalian sistem informasi perlu dikembangkan untuk memaastikan entri data, pemrosesan, metode penyimpanan serta output informasi yang dihasilkan benar seperti yang direncanakan. Jadi

pengendalian sistem informasi dirancang untuk memonitor dan memelihara kualitas serta keamanan aktifitas-aktifitas input, pemrosesan, output, penyimpanan data. Gambar 10.16 berikut memperlihatkan contoh pengendalian sistem informasi, yang dirancang untuk memonitor dan memelihara kualitas dan keamanan aktifitas-aktifitas input, pemrosesan, output, penyimpanan data. Sebagai contoh, sistem informasi harus merekam data dengan benar kedalam aplikasi sistem bisnis, sehingga tidak terjadi "garbage in garbage out (GIGO)". Juga termasuk password dan kode-kode pengamanan, dan format-format tampilan.



Gambar 10.16 *Examples of Information system controls*

Auditing IT security. Manajemen keamanan TI harus secara berkala diperiksa atau diaudit oleh karyawan bagian internal audit atau auditor ekternal. Beberapa perusahaan mempekerjakan special auditor keamanan komputer. Audit ini akan mengevaluasi apakah alat keamanan dan manajemen yang mamadai telah diimplementasikan. Hal ini biasanya meliputi verifikasi akurasi dan integritas perangkat lunak yang digunakan, input dn output yang dihasilkan oleh berbagai aplikasi bisnis. Tujuan lain yang juga penting adalah untuk menguji integritas dari jejak audit aplikasi. Penelusuran ini dapat dimulai dengan munculnya transaksi bisnis sampai dengan menjadi dokumen transaksi atau laporan yang didukung oleh suatu aplikasi bisnis.

SIMPULAN

Teknologi informasi merupakan komponen utama dari keberhasilan bisnis suatu perusahaan saat ini, tetapi teknologi informasi juga merupakan sumberdaya penting yang perlu dikelola dengan baik.

Pada tahun-tahun awal komputasi, pengembangan komputer berskala besar (*mainframe*), jaringan komunikasi data, dan terminal-terminal interface, menyebabkan sentralisasi (*centralization)* dari perangkat keras dan perangkat lunak komputer, database, dan spesialisspesialis informasi pada tingkat perusahaan. Era berikutnya, pengembangan mini komputerdan micro komputer mempercepat tren *downsizing*, yang memperlihatkan kembalinya pendekatan desentralisasi (*decentralization*) oleh banyak perusahaan. Akhirnya tren focus pada membangun kontrol yang lebih terpusat atas pengelolaan sumber daya perusahaan TI, disamping masih melayani kebutuhan strategis unit bisnis, terutama e-bisnis mereka dan inisiatif e-commerce. Tren ini mengakibatkan terjadi pengembangan struktur organisasi TI yang campuran (hibrida) dengan kombinasi dua komponen yaitu komponen sentralisasi dan komponen desentralisasi.

Dalam beberapa tahun ini, isu-isu akses ke data global telah menjadi pokok kontraversi politik dan hambatan teknologi dalam operasi-operasi bisnis global menjadi lebih nyata dengan

perkembangan internet dan e-commerce. Aliran data bisnis terjadi lintas batas-batas negara melalui jaringan-jaringan telekomunikasi dari sistem-sistem informasi global. Banyak negara menganggapnya sebagai suatu pelanggaran karena data mengalir tanpa melalui bea masuk dan regulasi ekpor dan impor barang dan jasa.

Tujuan dari manajemen keamanan adalah untuk akurasi, integritas dan keamanan dari proses-proses dan semua sumberdaya dari sistem informasi. Dengan demikian, manajemen keamanan yang efektif harus dapat meminimumkan kesalahan, penipuan, dan kerugian-kerugian dalam sistem-sistem informasi yang sekarang ini interkoneksi dengan para pelanggannya, pemasoknya, dan stakeholder lainnya.

DAFTAR PUSTAKA

1. Marakas, George M and O'Brien, James A: Introduction to Information System ,16th, 2013.Chapter 14, pages 626-642; pages 645-667; Chapter 13, pages 566-594; pages 596623
2. http://www.outsorcingandoffshoring.com/
3. http://www.databasedesign-resource.com/project-management-failure.html
4. http://www.globalplatform.org/
5. http://www.quickmba.com/strategy/global/
6. http://www.acm.org/about/code-of-ethics
7. http://www.labs,idefense.com
8. http://www.pcworld.com/downloads/collection/collid,1525/files.html
9. http://www.networkmagazineindia.com/200211/guest.shtml