TANTANGAN DALAM HAL ETIKA DAN KEAMANAN

1

Ilustrasi Kasus Keamanan

Pihak yang tidak bertanggung-jawab:

– memodifikasi situs Internet.
– memanfaatkan kartu-kredit untuk belanja.
– memalsukan email.
– memalsukan transaksi e-commerce.
– membuat virus komputer.
– menyerang/memacetkan saluran internet.

Hal-hal yang "**teknis**" di atas, bersama yang "**non-teknis**" harus dipahami secara menyeluruh (holistik)

2

Isyu Keamanan Sistem Informasi

Keperluan Sistem Informasi

– penjaminan **INTEGRITAS** informasi.
– pengamanan **KERAHASIAN** data.
– pemastian **KESIAGAAN** sistem Informasi.
– pemastian **MEMENUHI** peraturan, hukum, dan bakuan yang berlaku.

3

Bidang / Domain Keamanan Sistem Informasi

Aspek keamanan Sistem Informasi sedemikian luasnya, sehingga dapat dibagi menjadi 11 bidang/domain/sudut pandang.

Ke-11 bidang ini bersifat universal, sehingga pada prinsipnya serupa untuk berbagai sistem operasi dan distribusi (distro).

Selintas yang "**ditinjau**" ialah itu-itu juga; namun dari sebelas sudut pandang yang berbeda!

4

11 Domain Keamanan :

Pelaksanaan Pengelolaan Keamanan (*Security Management Practices*).
Sistem dan Metodologi Pengendalian Akses (*Access Control Systems and Methodology*).
Keamanan Telekomunikasi dan Jaringan (*Telecommunications and Network Security*)
Kriptografi (*Cryptography*).
Model dan Arsitektur Keamanan (*Security Architecture & Models*).

5

Keamanan Pengoperasian (*Operations Security*).
Keamanan Aplikasi dan Pengembangan Sistem (*Application and Systems Development Security*).
Rencana Kesinambungan Usaha dan Pemulihan Bencana (*Disaster Recovery and Business Continuity Plan -- DRP/BCP*).
Hukum, Investigasi, dan Etika (*Laws, Investigations and Ethics*).
Keamanan Fisik (*Physical Security*).
Audit (*Auditing*).

6

1. Pelaksanaan Pengelolaan Keamanan

Mempelajari:
– mengidentifikasi asset (informasi) perusahaan
– menentukan tingkat pengamanan asset tersebut
– menaksir anggaran keamanan yang diperlukan
– menyelaraskan antara anggaran yang tersedia dengan asset yang akan dilindungi.

7

2. Sistem dan Metodologi Pengendalian Akses

Mempelajari:
– mekanisme/metode pengendalian akses
– identifikasi, otentifikasi dan otorisasi
– pemantauan penggunaan sistem

8

3. Keamanan Telekomunikasi dan Jaringan

Mempelajari:
– teknologi dan protokol jaringan
– perangkat jaringan terkait
– aspek keamanan terkait yang terkait

9

4. Kriptografi

Mempelajari:
– metoda dan teknik penyembunyian

10

5. Model dan Arsitektur Keamanan

Prinsip-prinsip
– hak minimum (*least previlage*)
– pertahanan berlapis (*defense in depth*)
– pembatasan gerbang (*choke point*)
– titik terlemah (*weakest link*)
– pengamanan kegagalan (*fail-safe stance*)
– partisipasi total (*universal participation*)
– aneka pertahanan (*diversity of defense*)
– kesederhanaan (*simplicity*)

11

6. Keamanan Pengoperasian

Cakupan
– pemisahan tugas dan wewenang
– alur pertanggung-jawaban (*accountability*)
– perekrutan Sumber Daya Manusia
– pengendalian keluaran/masukan
– pengendalian pengelolaan perubahan
– penyerangan (*attack*)
– penyusupan (*intrusion*)
– penanggulangan virus

12

7. Keamanan Aplikasi dan Pengembangan Sistem

Cakupan:
– Tingkatan Kerumitan Fungsi dan Aplikasi
– Data
– Pengelolaan Keamanan BasisData
– SDLC: Systems Development Life Cycle
– metodology pengembangan aplikasi
– pengendalian perubahan perangkat lunak
– program bermasalah

13

8. Rencana Kesinambungan Usaha dan Pemulihan Bencana

Cakupan:
– Indentifikasi Sumber Daya Bisnis
– Penentuan Nilai Bisnis
– Analisa Kegagalan (*impact*) Bisnis (BIA)
– Analisa Kerugian
– Pengelolaan Prioritas dan Krisis
– Rencana Pengembangan
– Rencana Implementasi
– Rencana Pemeliharaan

14

9. Hukum, Investigasi, dan Etika

Cakupan:
– Hukum, Aturan, dan Etika
– Transaksi Elektronis
– Hak Kekayaan Intelektual
– Pembajakan
– Undang-undang keamanan dan eksport
– Penyelidikan Kejahatan Komputer
– Privasi

15

10. Keamanan Fisik

Cakupan:
– Kawasan Terbatas
– Kamera Pemantau dan Detektor Pergerakan
– Bunker (dalam tanah)
– Pencegahan dan Pemadaman Api
– Pemagaran
– Peralatan Keamaman
– Alarm
– Kunci Pintu

16

11. Audit

Cakupan:
– Rencana Audit
– Kendali
– Tujuan Kendali
– Metoda Audit
– Testing
– Pengumpulan Bukti
– Teknik Audit Berbantuan Komputer

17

11

Security and
Ethical Challenges
of e-Business

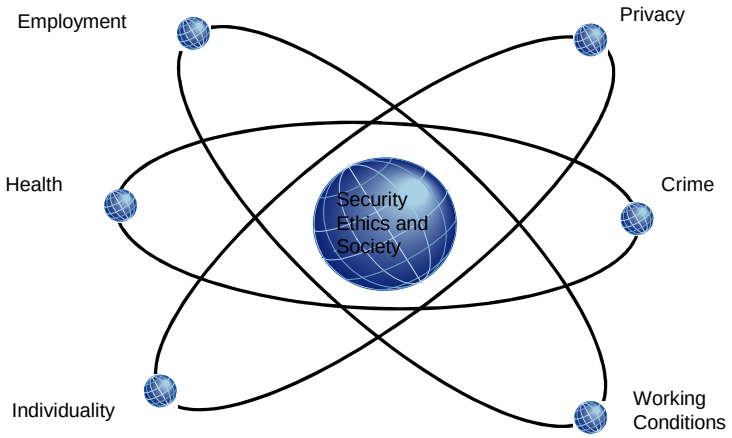
Chapter Objectives

- **Identify several ethical issues in how the use of information technologies in e-business affects employment, individuality, working conditions, privacy, crime, health, and solutions to societal problems.**
- **Identify several types of security management strategies and defenses, and explain how they can be used to ensure the security of e-business applications.**

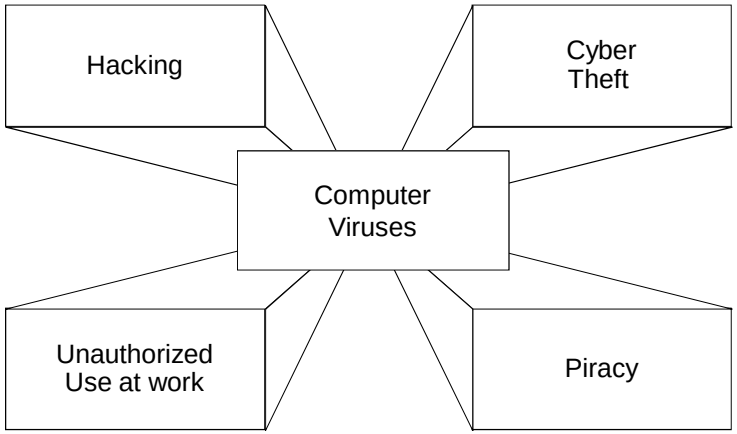
Chapter Objectives

- **Propose several ways that business managers and professionals can help to lessen the harmful effects and increase the beneficial effects of the use of information technology.**

Security and Ethical Challenges



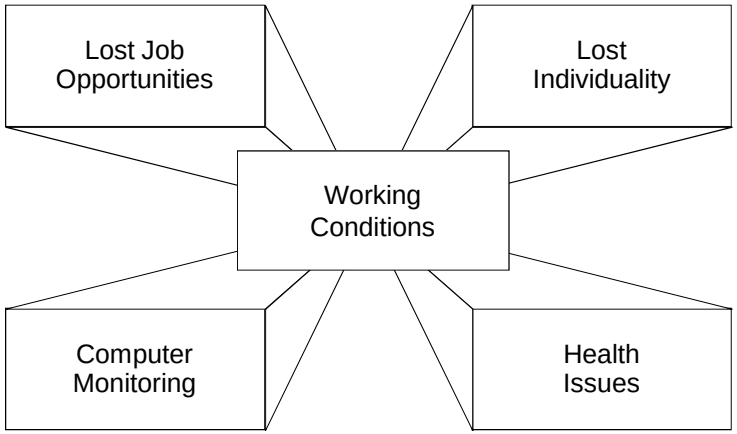
Computer Crime



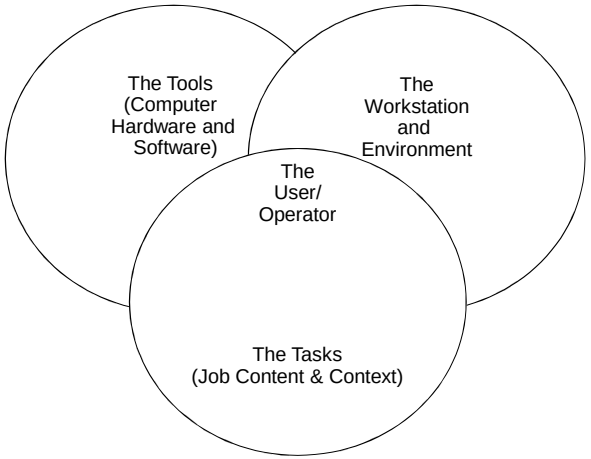
Common Hacking Tactics

- Denial of Service
- Scans
- Sniffer Programs
- Spoofing
- Trojan Horse
- Back Doors
- Malicious Applets
- War Dialing
- Logic Bombs
- Buffer Overflow
- Password Crackers
- Social Engineering
- Dumpster Driving

Employment Challenges



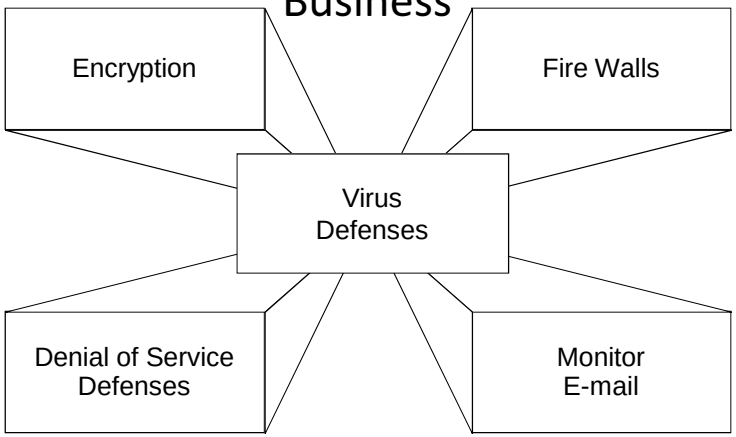
Ergonomic Factors in the Workplace



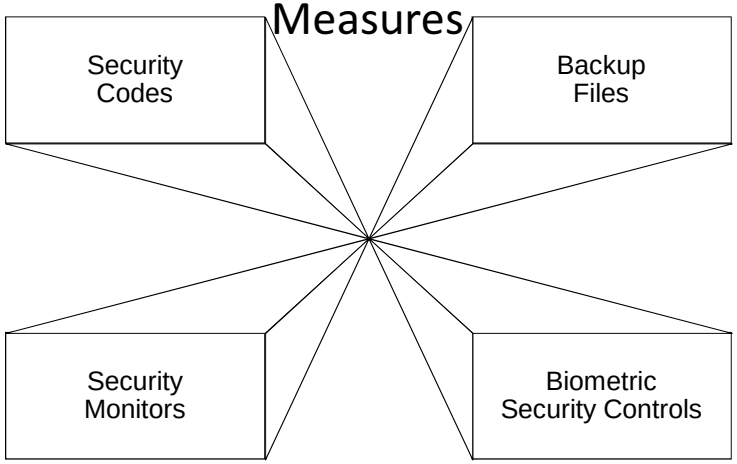
Ethical Considerations

- Ethical Principles
  - Proportionality
  - Informed Consent
  - Justice
  - Minimized Risk
- Standard of Conduct
  - Act with integrity
  - Protect the privacy and confidentiality of information
  - Do not misrepresent or withhold information
  - Do not misuse resources
  - Do not exploit weakness of systems
  - Set high standards
  - Advance the health and welfare of general public

Security Management of e-Business



Other e-Business Security Measures



Computer System Failure Controls

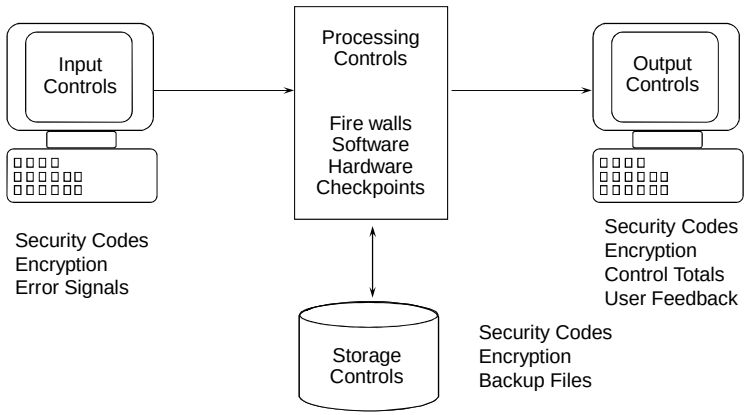
Fault Tolerant Systems
Fail-Over Fail-Safe Fail-Soft

Layer	Threat	Fault Tolerant Methods
Applications	**Environmental, HW and SW Faults**	Application redundancy, Checkpoints
Systems	**Outages**	System isolation Data security
Databases	**Data errors**	Transaction histories, backup files
Networks	**Transmission errors**	Alternate routing, error correcting routines
Processes	**HW and SW faults**	Checkpoints
Files	**Media Errors**	Replication of data
Processors	**HW Faults**	Instruction retry

Disaster Recovery

- Who will participate?
- What will be their duties?
- What hardware and software will be used?
- Priority of applications to be run?
- What alternative facilities will be used?
- Where will databases be stored?

e-Business System Controls and Audits



Chapter Summary

- **The vital role of e-bBusiness and e-commerce systems in society raises serious ethical and societal issues in terms of their impact on employment, individuality, working conditions, privacy, health, and computer crime.**
- **Managers can help solve the problems of improper use of IT by assuming their ethical responsibilities for ergonomic design, beneficial use, and enlightened management of e-business technologies in our society.**

Chapter Summary (cont)

- **Business and IT activities involve many ethical considerations. Ethical principles and standards of conduct can serve as guidelines for dealing with ethical businesses issues.**
- **One of the most important responsibilities of the management of a company is to assure the security and quality of its e-business activities.**
- **Security management tools and policies can ensure the accuracy, integrity, and safety of e-business systems and resources.**

ADA PERTANYAAN ?

34