"SAFEGUARDING" SUMBER DAYA INFORMASI

Perusahaan mengatasi kriminalitas komputer dengan menerapkan keamanan sistem (systems security) dan meminimisasi kerusakan akibat segala macam ancaman melalui ***contingency planning***.

KEAMANAN SISTEM (*SYSTEMS SECURITY*)

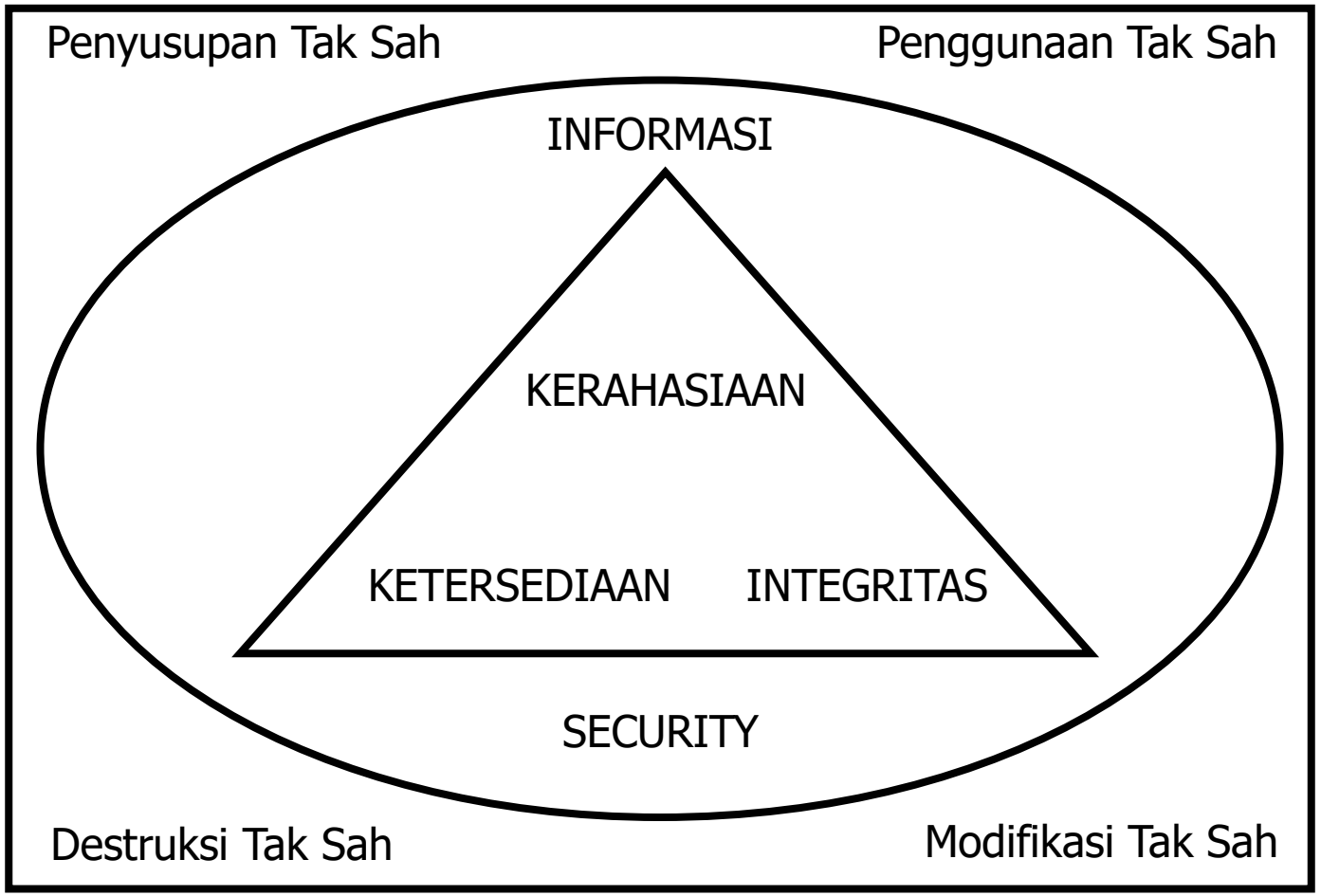
- Keamanan sistem ialah proteksi untuk segala sumber daya informasi dari penggunaan pihak-pihak yang tak berwenang.
- Perusahaan menerapkan *systems security* yang efektif dengan cara mengidentifikasi sumber daya informasi yang rawan gangguan dan menerapkan tolok ukur & cara pengamanan.
- Minat terhadap *systems security* makin meningkat karena beberapa alasan berikut ini:
  a. Operasi kritis/penting perusahaan sangat tergantung pada sistem informasi.
  b. Aplikasi *electronic data interchange* (EDI) memungkinkan organisasi untuk mengakses sumber daya informasi perusahaan yang berharga.
  c. Sistem saat ini umumnya memiliki akses *online* dari user yang berlokasi di seluruh perusahaan.
  d. Kebanyakan *end user* umumnya lalai dalam mengamankan dan menjaga sistem.

TUJUAN KEAMANAN

- Systems security diarahkan untuk mencapai tiga tujuan utama, yaitu kerahasiaan, ketersediaan, dan integritas.
  - Kerahasiaan (*confidentiality*).
    - Perusahaan berupaya melindungi data & informasi dari penyusupan orang yang tak berwenang.
    - Sistem Informasi Sumberdaya Manusia (HRIS) bertanggung jawab terhadap informasi tentang kepegawaian.
    - Sistem-sistem lainnya seperti *account receivable*, *purchasing*, dan *account payable* bertanggung jawab menjaga rahasia perorangan dari elemen-elemen lingkungan perusahaan.

- Ketersediaan (*availability*).
  - Tujuan sistem informasi berbasis komputer (CBIS) ialah menyediakan data dan informasi untuk orang-orang yang berwenang menggunakannya.
  - Tujuan ini sangat penting terutama untuk subsistem-subsistem pada CBIS yang berorientasi informasi.
- Integritas (*Integrity*).
  - Semua subsistem pada CBIS harus menyediakan refleksi akurat dari sistem fisik yang diwakilinya.

Tindakan Tak Sah Mengancam Tujuan System Security



CONTINGENCY PLAN

- Operasi komputer yang tidak terganggu oleh kriminal komputer atau bencana alam akan dapat dicapai melalui eksekusi strategi-strategi yang telah direncanakan sebelumnya.
- Perencanaan ini disebut sebagai disaster planning atau sekarang lebih dikenal sebagai *contingency planning*.
- Teknik yang lebih dipercaya perusahaan ialah membuat beberapa subplan yang berkaitan dengan *contingency*, yaitu *EMERGENCY PLAN, BACKUP PLAN*, dan *VITAL RECORDS PLAN*.
- Organisasi *information services* skala besar memiliki *manager of contingency planning* yang tugas utamanya ialah *contingency planning*.

EMERGENCY PLAN

- *Emergency plan* menetapkan pengukuran-pengukuran untuk keselamatan pegawai saat terjadi bencana, diantaranya yaitu:
    - sistem alarm,
    - prosedur evakuasi, dan
    - *fire suppression systems.*

BACKUP PLAN

Perusahaan harus mengatur backup fasilitas computing agar dapat digunakan saat terjadi kerusakan atau musnah. Backup dilakukan melalui kombinasi *REDUNDANCY, DIVERSITY*, dan *MOBILITY*.

a. *REDUNDANCY*. *Hardware*, *software*, dan data dibuat duplikasinya agar pada saat 'down' dapat digunakan backup-nya sehingga prosesing tidak terhenti.

b. *DIVERSITY*. Sumberdaya informasi tidak seluruhnya diinstall pada lokasi yang sama. Perusahaan besar umumnya memisahkan pusat *computing* untuk area operasi yang berbeda.

c. *MOBILITY*. Perusahaan-perusahaan kecil bekerja sama menyediakan backup dengan user lainnya yang memiliki tipe peralatan yang sama. Perusahaan besar dapat memobilitaskan pusat computingnya dengan mengontrakkan sumberdayanya untuk jasa backup secara hot site atau cold site.

- *HOT SITE* ialah fasilitas computing lengkap yang disediakan suplier untuk konsumennya untuk digunakan pada saat darurat.
- *COLD SITE*, sering disebut empty shell, perusahaan menyediakan site terpisah dari main *computing facility* dan hanya menyediakan fasilitas bangunan saja tanpa komputer. Komputernya sendiri diperoleh dari supplier dan diinstall pada empty shell.

VITAL RECORDS PLAN

- *Record-record vital* perusahaan ialah dokumentasi tercetak, *microform*, dan *magnetic storage media* yang diperlukan untuk menjalankan bisnis.
- *Record-record* pada *computer site* harus dijaga, selain itu *backup copies* pada *remote location* juga harus tersedia.
- Semua tipe *record* secara fisik dapat dtransportasikan ke *remote location* atau ditransfer secara elektronik

- Tiga jenis *electronic transmission service* yang tersedia ialah:

  1. *ELECTRONIC VAULTING*, mulai digunakan tahun 1988, ialah transmisi elektronik file-file backup secara *batch*.

  2. *REMOTE JOURNALING* mirip dengan *electronic vaulting* tetapi transmisi hanya dilakukan saat transaksi terjadi.

  3. *DATABASE SHADOWING* yaitu duplikasi *database* pada *remote sites* yang dijaga tetap *up-to-date*.

PENTINGNYA ETIKA

1. ETIKA SEBAGAI PARAMETER PERILAKU
2. EMPAT ISYU ETIKA
3. PERJANJIAN SOSIAL PENGGUNAAN KOMPUTER

ETIKA SEBAGAI PARAMETER PERILAKU

- Perilaku manusia dituntun oleh hukum, moral, dan etika.
    - Hukum terlihat jelas karena biasanya tertulis;
    - moral ialah standard betul atau salah yang secara umum dapat diterima; sedangkan
    - etika ialah ekspresi moral dalam bentuk aturan-aturan yang digunakan sebagai panduan.
- Beberapa aturan etika bersifat informal (diperoleh berdasarkan pengalaman), beberapa aturan lainnya bersifat formal yaitu didokumentasikan secara tertulis.

Organisasi-organisasi professional computing telah membuat lima aturan etika yaitu:

Nama Organisasi	Etika
Association for Computing Machinery	Professional Conduct and Procedures for the Enforcement of the ACM Code
Data Processing Management Association (DPMA)	Code of Ethics, Standards of Conduct and Enforcement Procedures
British Computer Society (BCS)	Code of Conduct
The Institute of Electrical and Electronics Engineers (IEEE)	Code of Ethics
The Institute for Certification of Computer Professionals (ICCP)	Codes of Ethics and Good Practices

EMPAT ISYU ETIKA

- Prof. Richard O'Mason (Southern Methodist University) mengidentifikasi empat isyu etika (diakronimkan sebagai PAPA) berkenaan dengan era informasi.
- PAPA, akronim dari
  - PRIVACY,
  - ACCURACY,
  - PROPERTY, dan
  - ACCESSIBILITY,

1. PRIVACY. Informasi apa yang berkaitan dengan seseorang atau asosiasi yang boleh diungkapkan kepada orang lain; pada kondisi apa dan dengan perlindungan apa? Apa yang boleh tetap dirahasiakan seseorang yang tidak dipaksa untuk diungkapkan kepada orang lain?
2. ACCURACY. Siapa yang bertanggung jawab terhadap otentik, kebenaran, dan akurasi (ketepatan) informasi? Siapa yang bertanggung jawab akibat error informasi dan bagaimana korban menerimanya?
3. PROPERTY. Siapa yang memiliki informasi? Apa dan berapa nilai tukar yang pantas? Siapa yang memiliki saluran transmisi informasi? Bagaimana akses ke sumberdaya yang jarang (scarce) ini dialokasikan?
4. ACCESSIBILITY. Informasi apa yang seseorang/organisasi mempunyai hak memeprolehnya, pada kondisi apa dan dengan perlindungan apa?

PERJANJIAN SOSIAL PENGGUNAAN KOMPUTER

- Lima prinsip dasar (Prof. Richard O'Mason) agar teknologi informasi dan informasi yang tanganinya digunakan untuk meningkatkan harkat hidup manusia. Perusahaan harus memenuhi perjanjian sosial penggunaan komputer dengan cara memastikan bahwa informasi sistem perusahaan:
    - tidak akan melanggar privacy seseorang.
    - Akurat.
    - melindungi penyalahgunaan transmisi sumberdaya informasi.
    - melindungi intellectual property.
    - dapat diakses untuk menghindari penghinaan information illiteracy & pencabutan HAM.