MATA KULIAH ISU SOSIAL DAN KEPROFESIAN TEKNOLOGI INFORMASI
KODE MATA KULIAH CCI410

DISUSUN OLEH
NIZIRWAN ANWAR & TEAM

FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL
JAKARTA
2018

MATERI

"PRIVACY AND SECURITY"

(PRIVASI DAN KEAMANAN)

4.1 PENDAHULUAN

Etika merupakan kepercayaan tentang hal yang benar dan salah atau yang baik dan yang tidak baik. Etika pertama kali dibahas dalam SI oleh Richard Mason (1986), yang mencakup PAPA, yaitu :

1) Privasi **PRIVASI** menyangkut hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang memang tidak diberi izin untuk melakukannya.

2) Akurasi **AKURASI** terhadap informasi merupakan faktor yang harus dipenuhi oleh sebuah sistem informasi. Ketidakakurasian informasi dapat menimbulkan hal yang menggangu, merugikan, dan bahkan membahayakan. Adapun contoh kasus, yaitu : a. terhapusnya nomor keamanan sosial yang dialami oleh Edna Rismeller (Alter, 2002, hal. 292). b. Kasus kesalahan pendeteksi misil Amerika Serikat.

3) Properti Perlindungan terhadap hak **PROPERTI** yang sedang digalakkan saat ini yaitu yang dikenal dengan sebutan HAKI (hak atas kekayaan intelektual).

   HAKI biasa diatur melalui hak cipta (copyright), paten, dan rahasia perdagangan (trade secret).

   a) Hak cipta adalah hak yang dijamin oleh kekuatan hukum yang melarang penduplikasian kekayaan intelektual tanpa seizin pemegangnya. Hak seperti ini mudah untuk didapatkan dan diberikan kepada pemegangnya selama masa hidup penciptanya plus 70 tahun.

   b) Paten merupakan bentuk perlindungan terhadap kekayaan intelektual yang paling sulit didapatkan karena hanya akan diberikan pada penemuan-penemuan inovatif dan sangat berguna. Hukum paten memberikan perlindungan selama 20 tahun.

   c) Hukum rahasia perdagangan melindungi kekayaan intelektual melalui lisensi atau kontrak. Pada lisensi perangkat lunak, seseorang yang menandatangani kontrak menyetujui untuk tidak menyalin perangkat lunak tersebut untuk diserahkan pada orang lain atau dijual.

   Berkaitan dengan kekayaan intelektual, banyak masalah yang belum terpecahkan (Zwass, 1998); antara lain:

   a) Pada level bagaimana informasi dapat dianggap sebagai properti?

   b) Apa yang harus membedakan antara satu produk dengan produk lain

   c) Akankah pekerjaan yang dihasilkan oleh komputer memiliki manusia penciptanya?

   d) Jika tidak, lalu hak properti apa yang dilindunginya?

4) Akses Fokus dari masalah **AKSES** adalah pada penyediaan akses untuk semua kalangan. Teknologi informasi diharapkan malah tidak menjadi halangan dalam melakukan pengaksesan terhadap informasi bagi kelompok orang tertentu, tetapi justru untuk mendukung pengaksesan untuk semua pihak.

4.2 KEAMANAN SISTEM INFORMASI

Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi. Tujuannya adalah untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem. Ancaman terhadap sistem informasi dapat dibagi menjadi dua macam, yaitu :

1) Ancaman aktif mencakup kecurangan dan kejahatan terhadap komputer.

2) Ancaman pasif mencakup kegagalan sistem, kesalahan manusia, dan bencana alam.

Metode yang umum digunakan oleh orang dalam melakukan penetrasi terhadap sistem berbasis komputer ada 6 macam (Bodnar dan Hopwood, 1993), yaitu

1) Pemanipulasian masukan

2) Penggantian program

3) Penggantian berkas secara langsung

4) Pencurian data

5) Sabotase

6) Penyalahgunaan dan pencurian sumber daya komputasi.

Teknik yang digunakan untuk melakukan hacking :

1) **Denial of Service (DoS)** ini dilaksanakan dengan cara membuat permintaan yang sangat banyak terhadap suatu situs sehingga sistem menjadi macet dan kemudian dengan mencari kelemahan pada sistem si pelaku melakukan serangan terhadap sistem.

2) **Sniffer** ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi Internet, menangkap password atau menangkap isinya.

3) **Spoofing** Melakukan pemalsuan alamat e-mail atau Web dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti password atau nomor kartu kredit.

Adapun Penggunaan Kode yang jahat, meliputi :

1) Virus

2) Cacing (worm)

3) Bom waktu

4) Kuda Trojan

Untuk menjaga keamanan sistem informasi diperlukan pengendalian terhadap sistem informasi (kontrol) yang mencakup :

1) Kontrol Administrasi

   Mempublikasikan kebijakan kontrol yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi. Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk dalam hal ini adalah proses pengembangan sistem, prosedur untuk backup, pemulihan data, dan manajemen pengarsipan data.

2) Kontrol terhadap Pengembangan dan Pemeliharaan

   Sistem Melibatkan Auditor sistem, dari masa pengembangan hingga pemeliharaan sistem, untuk memastikan bahwa sistem benar-benar terkendali, termasuk dalam hal otorisasi pemakai sistem. Aplikasi dilengkapi dengan audit trail sehingga kronologi transaksi mudah untuk ditelusuri.

3) Kontrol Operasi Tujuannya agar sistem beroperasi sesuai dengan yang diharapkan. Termasuk dalam hal ini:

   a) Pembatasan akses terhadap pusat data

   b) Kontrol terhadap personel pengoperasi

   c) Kontrol terhadap peralatan (terhadap kegagalan)

   d) Kontrol terhadap penyimpan arsip

   e) Pengendalian terhadap virus

4) Perlindungan Fisik terhadap Pusat Data

   Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar. Untuk mengantisipasi kegagalan sumber daya listrik, biasa digunakan UPS dan mungkin juga penyediaan generator.

5) Kontrol Perangkat Keras

Untuk mengantisipasi kegagalan sistem komputer, terkadang organisasi menerapkan sistem komputer yang berbasis fault-tolerant (toleran terhadap kegagalan). Toleransi terhadap kegagalan pada penyimpan eksternal antara lain dilakukan melalui disk mirroring atau disk shadowing, yang menggunakan teknik dengan menulis seluruh data ke dua disk secara parallel.

6) Kontrol Akses terhadap Sistem Komputer

Setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan password. Penggunaan teknologi yang lebih canggih menggunakan sifat-sifat biologis manusia yang bersifat unik, seperti sidik jari dan retina mata, sebagai kunci untuk mengakses sistem.

7) Kontrol terhadap Bencana

Rencana darurat (emergency plan) menentukan tindakan-tindakan yang harus dilakukan oleh para pegawai manakala bencana terjadi. Rencana cadangan (backup plan) menentukan bagaimana pemrosesan informasi akan dilaksanakan selama masa darurat. Rencana pemulihan (recovery plan) menentukan bagaimana pemrosesan akan dikembalikan ke keadaan seperti aslinya secara lengkap, termasuk mencakup tanggung jawab masing-masing personil. Rencana pengujian (test plan) menentukan bagaimana komponen-komponen dalam rencana pemulihan akan diuji atau disimulasikan.

8) Kontrol terhadap Perlindungan Terakhir

a) Rencana pemulihan dari bencana

b) Asuransi

4.3 ISU KEAMANAN DATA DAN INFORMASI

4.3.1 PRIVASI

- ✓ Informasi apa yang dapat diungkapkan seseorang kepada pihak lain? ‰
- ✓ Pemeriksaan seperti apa yang dapat digunakan perusahaan bagi para karyawannya? ‰
- ✓ Hal apa saja yang harus dirahasiakan oleh seseorang dan tidak diungkapkan ke pihak lain? ‰

- ✓ Informasi tentang seseorang yang harus disimpan di basis data, dan seberapa aman informasi tersebut di sana?

4.3.2 AKURASI

- ✓ Siapa yang bertanggung jawab terhadap autentika, kesesuaian dan akurasi informasi yang dikumpulkan? ‰
- ✓ Bagaimana cara memastikan informasi akan diproses secara tepat dan disajikan dengan akurat ke para pengguna? ‰
- ✓ Bagaimana cara memastikan berbagai kesalahan dalam basis data, transmisi data dan pemrosesan data bersifat disengaja atau tidak disengaja? ‰
- ✓ Siapa yang bertanggung jawab atas berbagai kesalahan dalam informasi, dan kompensasi apa yang harus diberikan pada pihak yang dirugikan?

4.3.3 PROPERTI

- ✓ Siapa yang memiliki informasi tersebut? ‰
- ✓ Berapakah harga yang tepat dan wajar untuk pertukarannya? ‰
- ✓ Bagaimana seharusnya menangani pembajakan peranti lunak? ‰
- ✓ Dapatkah seseorang menggunakan basis data dalam keadaan terpaksa? ‰
- ✓ Dapatkah komputer perusahaan digunakan untuk tujuan pribadi? ‰
- ✓ Bagaimanakah kompensasi diberikan kepada para pakar yang mengkontribusikan kepakarannya untuk membuat sistem pakar? ‰
- ✓ Bagaimana seharusnya akses ke berbagai saluran informasi dialokasinya?

4.3.4 AKSESIBILITAS

- ✓ Siapa yang diijinkan untuk mengakses informasi? ‰

- ✓ Seberapa besar biaya yang dibebankan untuk mengijinkan akses ke informasi? ‰
- ✓ Bagaimana aksesibilitas ke komputer disediakan bagi karyawan dengan keterbatasan fisik? ‰
- ✓ Siapakah yang disediakan peralatan yang dibutuhkan untuk mengakses informasi? ‰
- ✓ Informasi apa yang menjadi hak atau keistimewaan untuk didapat seseorang atau perusahaan, dan dalam kondisi apa serta bagaimana pengamanannya?

4.4 KEBIJAKAN DAN PERLINDUNGAN TERHADAP PRIVASI

4.4.1 KEBIJAKAN PRIVASI

Pengumpulan Data;

‰

- ✓ Data individu dikumpulkan hanya jika tujuannya untuk memenuhi tujuan bisnis yang sah. ‰
- ✓ Data harus memadai, relevan dan tidak berlebihan dalam kaitannya dengan tujuan bisnis. ‰
- ✓ Setiap individu harus memberikan ijin sebelum data yang berkaitan dengan mereka dikumpulkan.

Akurasi Data; ‰

- ✓ Data sensitif yang dikumpulkan mengenai berbagai individu harus diverifikasi sebelum dimasukkan dalam basis data. ‰
- ✓ Data harus akurat dan selalu diperbarui. File harus tersedia sehingga dapat dipastikan bahwa data tersebut benar. ‰
- ✓ Jika terdapat ketidaksepakatan mengenai akurasi data, versi dari orang terkait harus diperhatikan dan dimasukkan dalam pengungkapan file-nya.

Kerahasiaan Data; ‰

- ✓ Prosedur keamanan komputer harus diimplementasikan untuk memberikan jaminan yang wajar dari pengungkapan data secara tidak sah.
- ✓ Prosedur tersebut harus meliputi pengukuran keamanan fisik, teknis dan administratif. ‰ Pihak ketiga seharusnya tidak diberikan akses data tanpa sepengetahuan atau ijin orang terkait, kecuali diminta oleh hukum. ‰
- ✓ Pengungkapan data, selain dari yang sangat rutin, harus diperhatikan dan dipelihara selama data disimpan. ‰
- ✓ Data seharusnya jangan diungkapkan untuk berbagai alasan yang tidak sesuai dengan tujuan bisnis, yang merupakan tujuan awal dikumpulkannya data tersebut.

4.4.2 PERLINDUNGAN PRIVASI

Privasi adalah hak untuk tidak diganggu dan hak bebas dari gangguan pribadi yang tidak wajar.

Privasi informasi adalah hak untuk menentukan kapan dan sejauh mana informasi mengenai diri sendiri dapat dikomunikasikan ke pihak lain. Salah satu cara untuk melindungi privasi adalah dengan mengembangkan kode etik atau kebijakan privasi.

Pemeriksaan elektronik adalah penelusuran aktivitas orang, secara online atau offline, dengan bantuan komputer. Informasi personal di berbagai basis data seperti bank dan lembaga keuangan; perusahaan TV kabel, telepon dan utilitas; perusahaan apartemen; pegadaian; persewaan; rumah sakit, sekolah dan universitas; supermarket, retail dan kurir; lembaga pemerintahan; perpustakaan; perusahaan asuransi dan lainnya.

Kode etik dan kebijakan privasi adalah petunjuk perusahaan yang berkaitan dengan perlindungan privasi para pelanggan, klien dan karyawan.

4.5 MANAJEMEN KEAMANAN DATA

Dalam bentuk yang paling dasar, manajemen keamanan informasi terdiri dari 4 tahap yaitu: mengidentifikasi ancaman yang dapat menyerang sumber informasi perusahaan; mengidentifikasi resiko yang mungkin ditimbulkan oleh ancaman tersebut; menetapkan kebijakan-kebijakan keamanan informasi; dan melaksanakan pengawasan terhadap hal-hal yang berhubungan dengan resiko keamanan

informasi. **Ancaman (*threat*)** dapat menimbulkan resiko yang harus dikontrol. Istilah **manajemen resiko** (***risk management***) dibuat untuk menggambarkan pendekatan secara mendasar terhadap resiko keamanan yang dihadapi oleh sumber-sumber informasi perusahaan.

Terdapat pilihan lain untuk memformulasikan kebijakan tentang keamanan informasi perusahaan. Pilihan tersebut menjadi populer pada tahun-tahun belakangan ini dengan kemunculan standar keamanan informasi atau benchmark. Benchmark merupakan salah satu tingkat kinerja yang diharapkan dapat dicapai dalam keamanan informasi perusahaan. *Benchmark* keamanan informasi merupakan suatu tingkat keamanan yang disarankan untuk perusahaan yang berada dalam keamanan normal.

Tingkat keamanan ini berupa perlindungan yang wajar dan dapat diterima terhadap gangguan dari luar perusahaan. Baik standar maupun benchmark keamanan, keduanya ditentukan oleh pemerintah dan asosiasi industri serta menunjukkan model keamanan yang dianggap dan diyakini pemerintah sebagai program keamanan informasi yang baik. Ketika sebuah perusahaan menggunakan pendekatan ini maka disebut pelaksanaan benchmark (***benchmark compliance***).

Pelaksanaan benchmark dilakukan perusahaan dengan asumsi bahwa pemerintah dan asosiasi industri telah mempertimbangkan dengan baik mengenai ancaman-ancaman dan resiko yang mungkin terjadi pada perusahaan dan benchmark dianggap dapat memberikan perlindungan yang baik. Gambar di atas menunjukkan pelaksanaan pendekatan benchmark.

4.6 ANCAMAN KEAMANAN DATA

Ancaman terhadap keamanan informasi berasal dari individu, organisasi, mekanisme, atau kejadian yang memiliki potensi untuk menyebabkan kerusakan pada sumber-sumber informasi perusahaan. Ketika kita berpikir tentang ancaman terhadap keamanan informasi, maka kita juga akan berpikir tentang aktivitas-aktivitas yang sengaja dilakukan individu-individu dan kelompok-kelompok di luar perusahaan.

Pada kenyataannya, ancaman dapat bersifat internal, yaitu berasal dari dalam perusahaan, maupun eksternal atau berasal dari luar perusahaan. Ancaman dapat juga terjadi secara sengaja atau tidak sengaja. Gambar di bawah memperlihatkan tujuan-tujuan keamanan informasi dan bagaimana tujuan tersebut sesuai dengan 4 tipe resiko yang dihadapi.

1) **Interuption:ancaman terhadap availability**, yaitu data dan informasi yang berada dalam system computer yang dirusak dan dibuang sehingga menjadi tidak ada atau menjadi tidak berguna.

2) **Interception merupakan ancaman terhadap secrey**, yaitu orang yang tidak berhak mendapatkan akses informasi dari dalam system computer

3) **Modification merupakan ancaman terhadap integritas**, yaitu orang yang tidak berhak, tidak hanya berhasil mendapatkan akses, melainkan juga dapat melakukan pengubahan terhadap informasi.

4) **Fabrication**: adanya orang yang tidak berwenang, meniru atau memalsukan suatu objek ke dalam system.

4.6.1 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.

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.

Terdapat 4 (empat) langkah yang diambil dalam mendefinisikan resiko, yaitu:

1) Identifikasi aset-aset bisnis yang harus dilindungi dari resiko.

2) Kenali resiko

3) Tentukan tingkat-tingkat dari dampak yang ditimbulkan resiko pada perusahaan.

4) Analisis kelemahan-kelemahan perusahaan

Untuk melengkapi analisis resiko, hal-hal yang ditemukan dalam analisis harus didokumentasikan dalam laporan analisis resiko. Untuk setiap resiko, isi laporan harus menyertakan informasi sebagai berikut

1) Deskripsi resiko

2) Sumberresiko

3) Tingkat kekuatan resiko

4) Kontrol yang diterapkan terhadap resiko

5) Pemilik resiko

6) Tindakan yang direkomendasikan ntuk menangani resiko

7) Batasan waktu yang direkomendasikan untuk menangani resiko.

8) Apa yang telah dilakukan untuk mengurangi resiko tersebut.

Tabel 1 Dampak terhadap Tingkat 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

4.6.2 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.

Tabel 2 *Malware Software*

Peranti Lunak yang berbahaya (Malicious Software-Malware)
1. 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
2. Worm Program yang tidak dapat mereplikasikan dirinya sendiri di dalam sistem, tetapi dapat menyebarkan salinannya melalui e-mail
3. Trojan Horse Program yang tidak dapat mereplikasi atau mendistribusikan dirinya sendiri, namun disebarkan sebagai perangkat
4. Adware Program yang memunculkan pesan-pesan yang mengganggu
5. Spyware Program yang mengumpulkan data dari mesin pengguna

4.6.3 ANCAMAN INTERNAL DAN EKSTERNAL

Ancaman bersifat internal tidak hanya berasal dari para pegawai tetap perusahaan tetapi dapat juga berasal dari para pegawai sementara, konsultan, kontraktor, dan rekan bisnis perusahaan

Survey yang dilakukan oleh suatu Institut Keamanan Komputer menemukan bahwa 49% responden menyatakan mengalami kejadian yang membahayakan keamanan informasi ternyata dilakukan pengguna yang sah dan diperkirakan 81 % kejahatan komputer dilakukan oleh pegawai perusahaan.

Ancaman yang berasal dari dalam perusahaan diperkirakan mempunyai bahaya yang lebih serius dibandingkan ancaman yang berasal dari luar perusahaan, karena individu dan kelompok internal memiliki pengetahuan yang lebih mengenai sistem yang ada di dalam perusahaan tersebut.

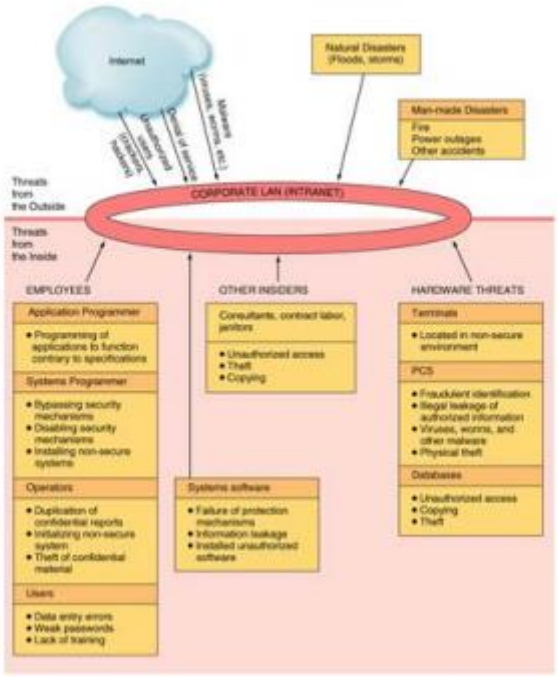
Kontrol yang dibuat untuk menghadapi **ancaman eksternal** biasanya baru mulai bekerja jika serangan terhadap keamanan terdeteksi. Sedangkan kontrol untuk menghadapi ancaman internal dibuat untuk memprediksi gangguan keamanan yang mungkin terjadi.

4.6.4 KESENGAJAAN DAN KETIDAK SENGAJAAN

Tidak semua ancaman berasal dari perbuatan yang disengaja dengan maksud untuk menimbulkan kerugian. Banyak diantaranya karena ketidaksengajaan atau kebetulan, baik yang berasal dari orang di dalam maupun luar perusahaan.

Dengan adanya hal seperti ini, maka keamanan informasi harus ditujukan tidak hanya untuk mengatasi ancaman yang timbul karena kesengajaan tetapi juga harus mampu mengurangi bahkan menghilangkan faktor-faktor yang dapat menimbulkan ancaman yang tidak disengaja terhadap keamanan perusahaan.

Lampiran Gambar



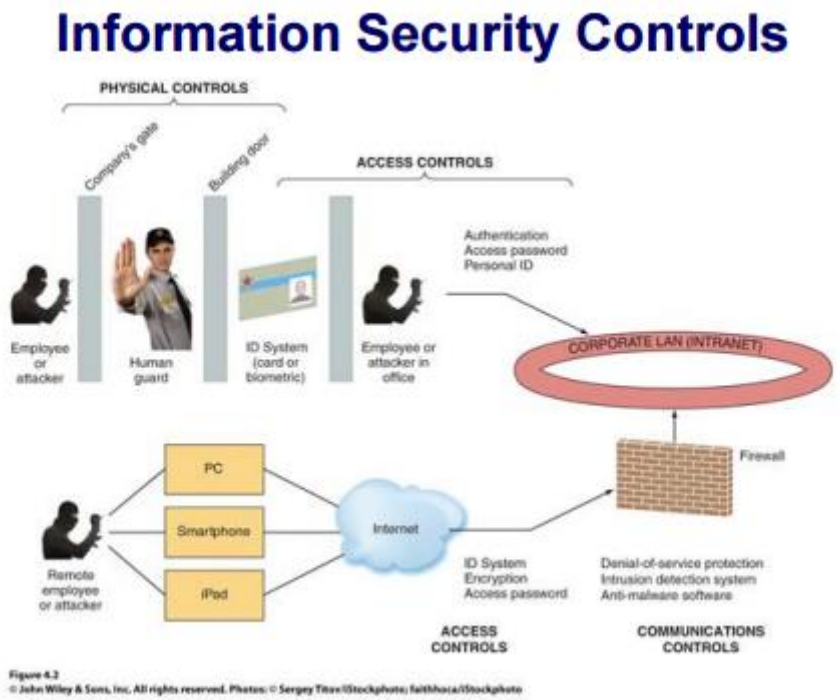


Figure 4.3

4.7. DAFTAR PUSTAKA

Mcleod Jr, Raymond, George P Schell.(2007). Management Information Systems.(10th Edition). USA: Pearson Prentice Hall.

Ibisa. 2011. Keamanan Sistem Informasi. Yogyakarta: CV Andi Offset

Rahardjo, Budi. 2005. Keamanan Sistem Informasi Berbasis Internet. Bandung: PT. Insan Indonesia