Chapter #4

Klasifikasi Aset dan Kendali Akses

AIK21363 (3 sks)

Keamanan dan Jaminan Informasi

Information Assurance and Security

Nurdin Bahtiar, M.T

Materi

1. Identifikasi aset
2. Kontrol terhadap infrastruktur IT
3. Peraturan manajemen tentang IT

1. Identifikasi aset

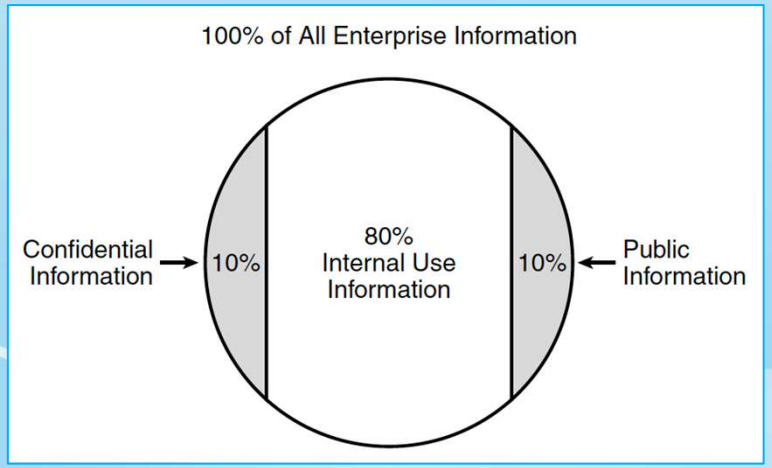
- Langkah ini dimulai dengan melakukan identifikasi dan inventarisasi aset perusahaan yang dalam hal ini terkait dengan fasilitas sistem informasi.
- Proses identifikasi dapat dilakukan dengan mengelompokkan aset-aset perusahaan ke dalam kelompok-kelompok atau beberapa kategori.
- Kategori pengelompokan tersebut dapat mengacu pada ISO/IEC 27002, 2005.

1. Identifikasi aset

- Kategori tersebut antara lain:
  - ✓ Aset informasi,
  - ✓ Aset perangkat lunak,
  - ✓ Aset perangkat keras,
  - ✓ Layanan atau service,
  - ✓ Prosedur,
  - ✓ Database maupun orang,
  - ✓ dan aset yang sifatnya *intangible benefit*, misalnya pamor perusahaan atau reputasi perusahaan.
- Seluruh aset tersebut dibuat dalam sebuah daftar aset perusahaan.

1. Identifikasi aset

- Perusahan mengklasifikasikan informasi untuk menetapkan tingkat perlindungan yang sesuai untuk sumber daya informasi ini.
- Karena sumber daya ini terbatas, perlu diprioritaskan dan diidentifikasi hal apa yang benar-benar membutuhkan perlindungan (lihat Gambar 1.1).
- Salah satu alasan untuk mengklasifikasikan informasi adalah untuk memastikan bahwa sumber daya yang langka ini seharusnya berada di tempat yang paling baik.



Gambar 1.1 Information Classification Breakdown

1. Identifikasi aset

- Beberapa contoh klasifikasi aset informasi:

Mega Oil Corporation

- HIGHLY CONFIDENTIAL — Information whose unauthorized disclosure will cause the corporation severe financial, legal, or reputation damage. Examples: acquisitions data, bid details, contract negotiation strategies.
- CONFIDENTIAL — Information whose unauthorized disclosure may cause the corporation financial, legal, or reputation damage. Examples: employee personnel and payroll files, competitive advantage information.
- GENERAL — Information that, because of its personal, technical, or business sensitivity, is restricted for use within the company. Unless otherwise classified, all information within Amoco is in this category.

Gambar 1.2 Information Classification Category (Example 1)

1. Identifikasi aset

Business Impact	*Classification Level*		
Maximum	1	2	3
Medium	2	2	3
Minimum	2	3	4

1: Availability safeguards must be implemented.
2: Availability safeguards should be implemented.
3: Continue to monitor availability requirements.
4: No additional action required at this time.

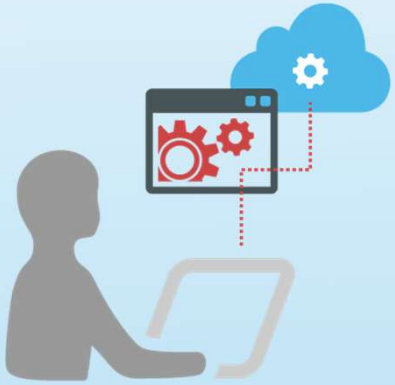
Gambar 1.3 Criticality Matrix

International Service Provider

- **Top Secret** — Information that, if disclosed, could cause severe impact to the company's competitive advantage or business strategies.
- **Confidential** — Information that, if disclosed, could violate the privacy of individuals, reduce competitive advantage, or damage the company.
- **Restricted** — Information that is available to a specific subset of the employee population when conducting company business.
- **Internal Use**— Information that is intended for use by all employees when conducting company business.
- **Public** — Information that has been made available to the public through authorized company channels.

Gambar 1.4 Information Classification Category (Example 2)

2. Kontrol terhadap infrastruktur IT



- Semua peningkatan terhadap teknologi informasi telah meningkatkan keuntungan bagi industri, namun di lain sisi telah menimbulkan masalah tambahan dan baru dari segi kontrol dan keamanan yang patut untuk diperhatikan.
- Persoalan kontrol yang patut untuk dipertimbangkan berkaitan dengan infrastruktur IT:
  - ✓ Peraturan pengadaan
  - ✓ Persoalan pengelolaan
  - ✓ Integritas sistem

2. Kontrol terhadap infrastruktur IT

1. Peraturan pengadaan barang

- Peraturan untuk pengadaan barang harus dibuat dan dirumuskan secara tertulis dan resmi.
- Prosedur administrasi untuk pengadaan ini harus diseragamkan, dipatuhi, dan diinformasikan kepada semua departemen. Apabila mungkin, pusatkan semua pembelian melalui departemen pembelian.
- Peraturan dan prosedur tersebut mencakup:
  - ✓ Justifikasi / pertimbangan yang kuat
  - ✓ Standardisasi
  - ✓ Supplier
  - ✓ Proses pengadaan

2. Kontrol terhadap infrastruktur IT

2. Persoalan pengelolaan

- Setelah pengadaan disetujui, langkah selanjutnya adalah mengontrol aktifitas yg akan dilakukan dengan infrastruktur tersebut.

- Persoalan pertama adalah menentukan sistem apa yang akan dikembangkan di infrastruktur tersebut. Bagi perusahaan yang memiliki komputer besar, penentuan harus dikembangkan secara kritis mengingat cara pengembangan sistem dengan menggunakan mesin besar agak berbeda dengan pengembangan sistem di PC.

- Persoalan lainnya adalah menentukan siapa yang membangun sistem baru tersebut. Dilakukan oleh ICT (atau pemakai sendiri) ataukah dilakukan oleh pihak ketiga. Apabila dilakukan oleh pihak ketiga, alangkah bergunanya apabila ICT tetap dilibatkan juga meskipun secara pasif. Karena ICT tetap berperan saat pasca pengembangan yang telah dilalui.

2. Kontrol terhadap infrastruktur IT

3. Integritas sistem

- Secara umum, PC memiliki control akses yang lebih lemah dibandingkan dengan mainframe. Terutama PC yang masih menggunakan sistem operasi DOS.
- Beberapa faktor yang menyebabkan masih digunakannya sistem operasi DOS:
  - ✓ Sudah cukup puas dengan aplikasi yang ada
  - ✓ Tidak tersedianya biaya yang cukup untuk pengembangan
  - ✓ SDM yang kurang tanggap dengan laju teknologi, dsb.
- Perusahaan tidak boleh berlaku pasif terhadap proteksi yang lemah terhadap arsip-arsip dan program PC serta kemudahan pengaksesan yang dilakukan oleh orang yang tidak berwenang.

2. Kontrol terhadap infrastruktur IT

- Selain itu, dengan berdirinya secara sendiri dan terpisah aplikasi akan menyebabkan terjadinya redundansi data, karena masing-masing PC memiliki data sendiri-sendiri. Cara bekerja seperti ini merupakan cara bekerja yang tidak efisien.
- Sistem operasi yang terbaru telah memiliki fitur yang dimiliki oleh mesin besar seperti pengaksesan harus memakai password, screen saver, dan sebagainya.
- Apabila PC yang memiliki resiko tinggi dan bersifat *stand alone*, akan lebih baik apabila *physical security* juga diterapkan misalnya meletakkan PC terkait di ruangan khusus / sendiri yang hanya dapat diakses oleh orang-orang tertentu sehingga dapat dikontrol penggunanya.

3. Peraturan manajemen tentang IT

- Adanya dampak terhadap serangan terhadap infrastruktur, seharusnya membuat manajemen dapat mengeluarkan peraturan demi melindungi aset digitalnya.
- Sudah sepatutnya salah satu peraturan yang harus dibuat dan dirumuskan secara tertulis dan resmi adalah mengenai penangkalan ancaman terhadap PC, beberapa contoh di antaranya:

1. Peraturan mengenai penggunaan internet atau email
2. Standar prosedur operasi untuk bagian ICT
3. Prosedur recovery
4. Prosedur pemeriksaan konfigurasi
5. Prosedur pemeriksaan mesin
6. Prosedur pemeriksaan terhadap ekstensi file yang tersembunyi.

End of File

Latihan

- Peraturan mengenai penangkalan ancaman terhadap PC di antaranya berisi 6 hal.
- Temukan dan ceritakan studi kasus yang terkait dengan salah satu isu tersebut
- Susunlah sebuah contoh standar operation procedure (SOP) yang berisi tentang cara mengatasi permasalahan tersebut. Gambarkan diagram swimlane-nya.
- Outline:
  - ✓ Nama perusahaan (include penjelasan bisnisnya)
  - ✓ Isu yang dikaji
  - ✓ Studi kasus (kejadian, akibat, penanggulangan)
  - ✓ SOP penyelesaian
  - ✓ Diagram swimlane.