Manajemen Keamanan TI

Managing Information Resources and Security

Oleh :
Saripudin

Prodi Pendidikan Manajemen Bisnis
Fakultas Ekonomi dan Manajemen
Universitas Pendidikan Indonesia
2008

LEARNING OBJECTIVES

- *After studying this chapter, you will be able to:*
  - Recognize the difficulties in managing information resources.
  - Understand the role of the IS department and its relationships with end users.
  - Discuss the role of the chief information officer.
  - Recognize information systems' vulnerability, attack methods, and the possible damage from malfunctions.
  - Describe the major methods of defending information systems.
  - Describe the security issues of the Web and electronic commerce.
  - Describe business continuity and disaster recoveryplanning.
  - Understand the economics of security and risk management.

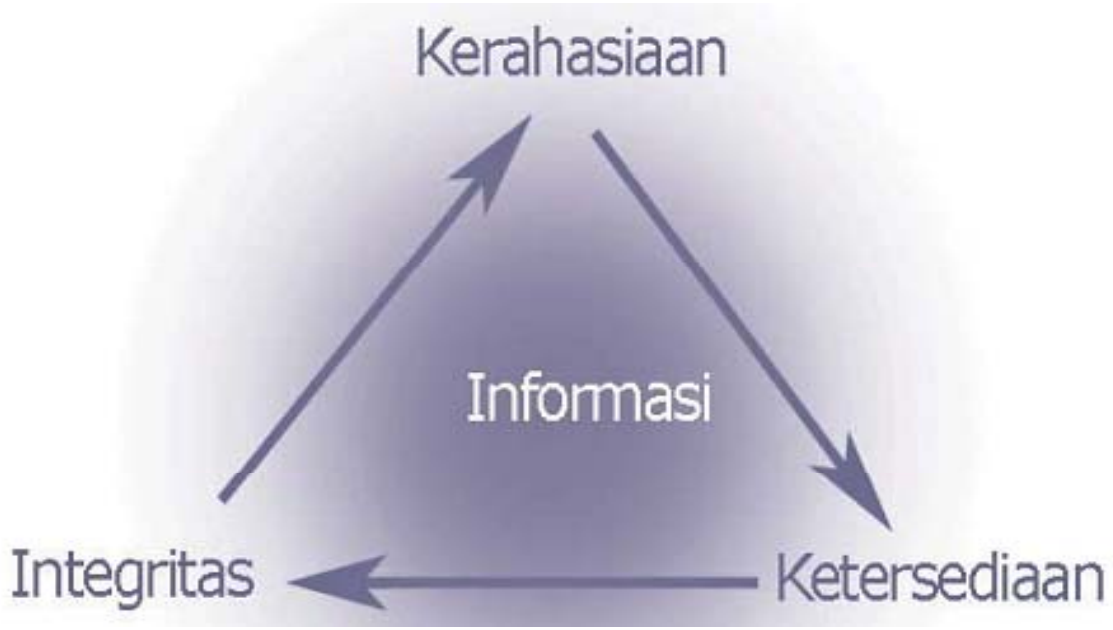
Apa itu Keamanan Informasi?

- Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:
  - *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
  - *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
  - *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).
  - Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

Sebelas Domain Keamanan

1. Security Management Practices
2. Access Control System & Methodology
3. Telecommunications & Network Security
4. Cryptography
5. Security & Architecture Models
6. Operations Security
7. Application & System Development Security
8. Disaster Recovery & Business Continuity Plan
9. Laws, Investigations & Ethics
10. Physical Security
11. Auditing

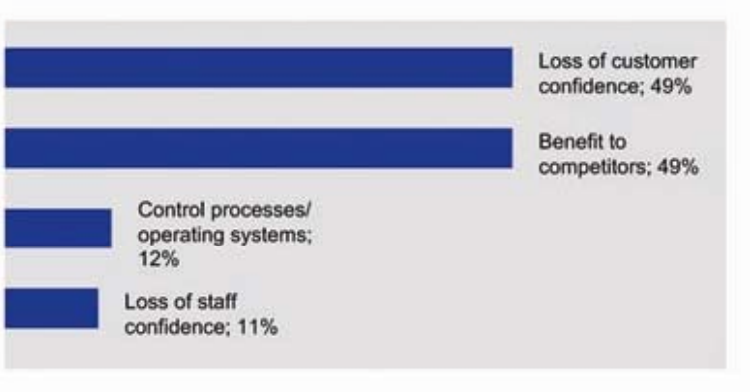
Elemen-elemen keamanan informasi

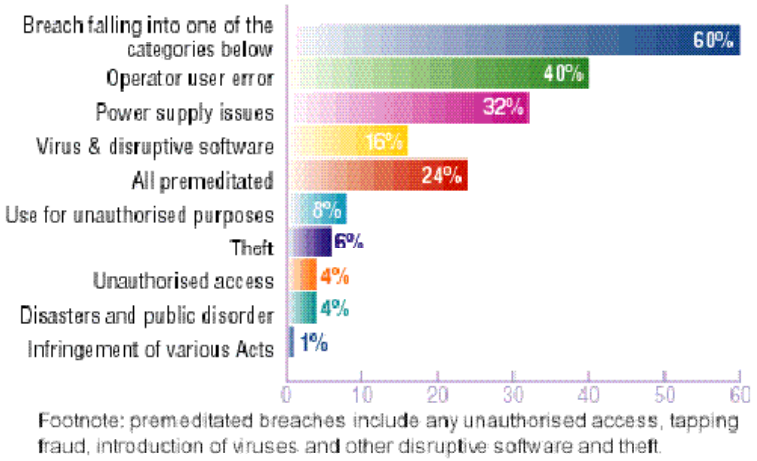


Mengapa diperlukan keamanan informasi?

- Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.
- Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara/terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:

Grafik persentase ancaman keamanan sistem informasi





Footnote: premeditated breaches include any unauthorised access, tapping fraud, introduction of viruses and other disruptive software and theft.

Lanjutan

- Survey tersebut juga menunjukkan bahwa 60% organisasi mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan. Kegagalan sistem keamanan lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Faktor internal ini diantaranya kesalahan dalam pengoperasian sistem (40%) dan diskontinuitas power supply (32%).
- Hasil survey ISBS tahun 2004-2006 menunjukkan bahwa terdapat banyak jaringan bisnis di Inggris (UK) telah mendapatkan serangan dari luar.

Apa Isi dari ISO-17799

- Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

THANKS

QUESTION and ANSWER

- Q : ?
- Q over by:..
  - A :....

Cybercrime in the New Millennium

- 15.1The IS Department and End Users
- 15.2The CIO in Managing the ISDepartment
- 15.3 IS Vulnerability and ComputerCrimes
- 15.4Protecting Information Resources: From National to Organizational Efforts
- 15.5Securing the Web, Intranets, and Wireless Networks
- 15.6 Business Continuity andDisaster Management
- 15.7 Implementing Security: Auditing and Risk Analysis

Minicases:

- (1) Home Depot /
- (2) Managing Security

- e-Based systems and computer networks are ubiquitous in the modern world, with applications spanning e-commerce, WLANs, healthcare and governmental organizations, amongothers. The secure transfer of information has therefore become a critical area of research,development, and investment.