

The Need for Disaster Recovery Center

Security Aspects

Budi Rahardjo

<http://budi.insan.co.id>

Oktober 2003



CIO/CTO top priorities for 2002

1. **Security**
2. ERP Implementation
3. **Disaster Recovery**
4. Web Development
5. Windows 2000
6. Storage

“Security is a top concern and a most likely spending area in 2002.”

Merrill Lynch Global Securities



Budi Rahardjo

Sumber Disater

- System Downtimes or Failures (72%)
- Inadvertent Errors (71%)
- Viruses (46%)
- Malicious Acts by Employees (29%)
- Malicious Acts by Outsiders (19%)
- Natural Disasters (17%)
- Unknown Source (15%)
- Industrial Espionage (8%)

Source : CSI Computer Crime and Security Survey (1999)

Budi Rahardjo

Mail Server Availability: Top Concern



Budi Rahardjo

Aspek Keamanan

- Privacy / Confidentiality
- Integrity
- **Availability**
- Non-repudiation
- Authentication
- Access control

Budi Rahardjo

Availability / Ketersediaan

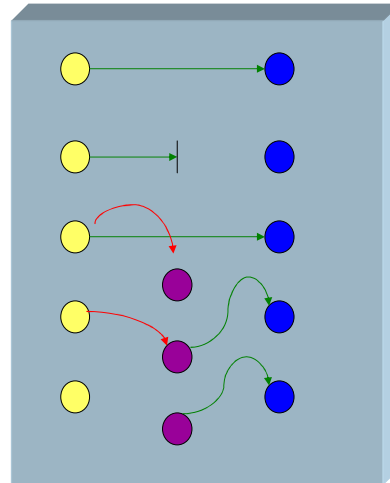
- (Sistem) Informasi harus dapat tersedia ketika dibutuhkan
 - Serangan terhadap server: dibuat hang, down, crash, lambat
 - Server bisa dicuri
 - Tempat terbakar
- Serangan: Denial of Service (DoS) attack

Budi Rahardjo

Tipe Ancaman

(threats)

- Normal flow
- Interruption
- Interception
- Modification
- Fabrication



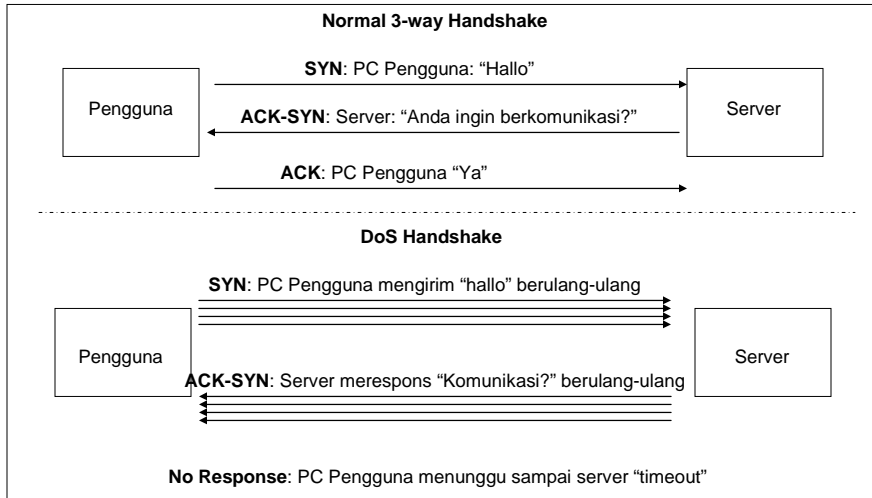
Budi Rahardjo

Interruption Attack

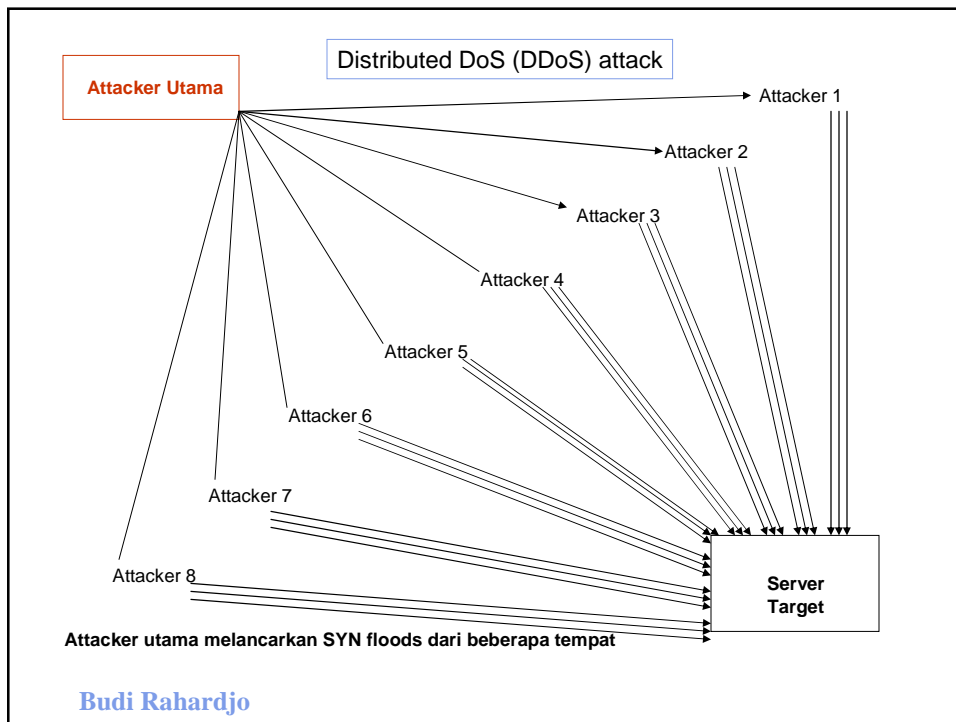
- Denial of Service (DoS) attack
 - Menghabiskan bandwidth, network flooding
 - Memungkinkan untuk memalsukan originating address
 - Tools: ping broadcast, smurf, synk4, macof, sky dance, dan flood utilities lainnya
- Proteksi:
 - Sukar jika kita sudah diserang
 - Filter at router for outgoing packet, filter attack originating from our site

Budi Rahardjo

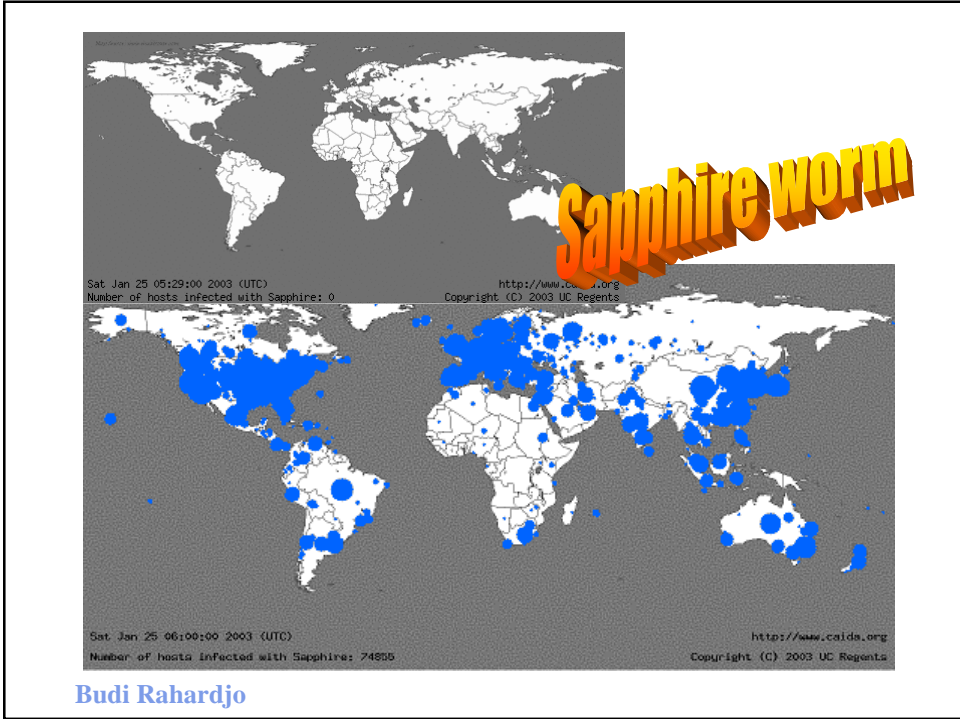
Network (DoS) SYN Attack



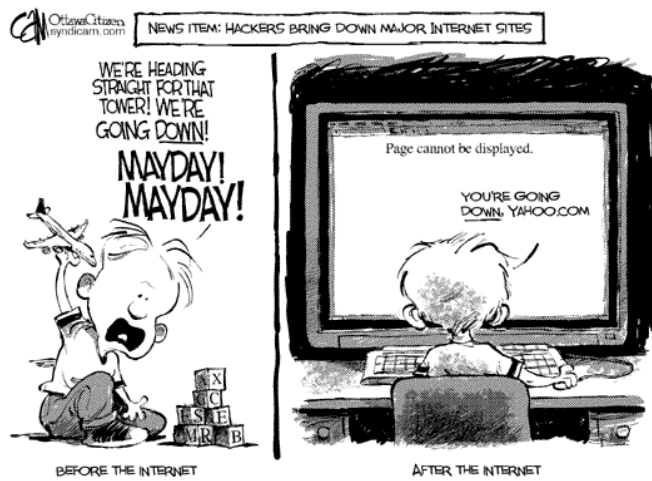
Budi Rahardjo



Budi Rahardjo



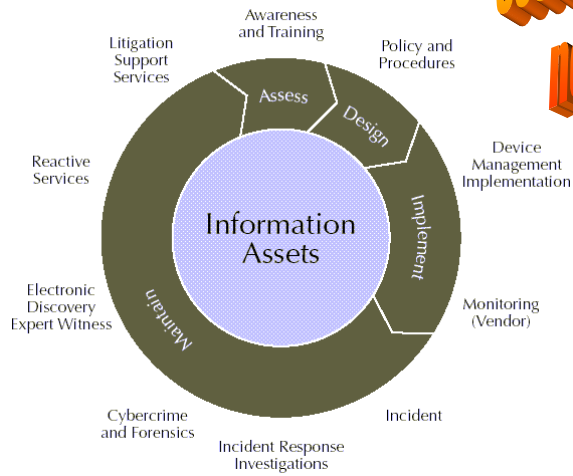
Serangan Hacker Kecil



Budi Rahardjo

Security Lifecycle

**Security is a process
not a product**



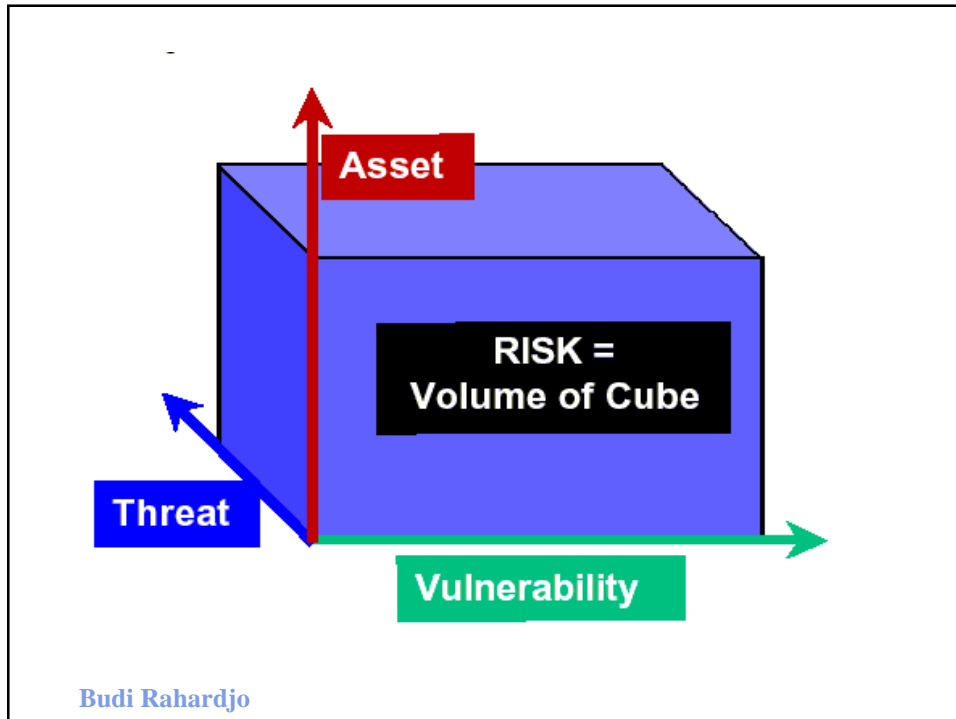
Budi Rahardjo

Asset & Value



- Apa yang ingin dilindungi?
 - Fisik (tangible): komputer, real money
 - Informasi (intangible): data-data rekening di Bank, confidential information, data kepegawaian, data gaji karyawan
 - Kepercayaan (trust) dan nama baik (intangible)
 - Manusia (life)
- Investasi di security melihat nilai dari aset yang ingin dilindungi

Budi Rahardjo



RISK



- RISK: “kemungkinan akan terjadinya suatu gangguan yang merugikan secara aktual”
- RISK: “suatu serangan yang mencapai satu atau lebih sasaran kunci yang sedang dikejar”
- RISK: “perubahan di masa depan yang mengarah pada situasi yang tidak dapat diterima”

Source: Dimitri Mahayana

Budi Rahardjo

RISK MANAGEMENT

Risk Exposure =



Probability of occurrence

X

Consequence of occurrence
(severity)

Budi Rahardjo

RISK MANAGEMENT



Risk Avoidance →

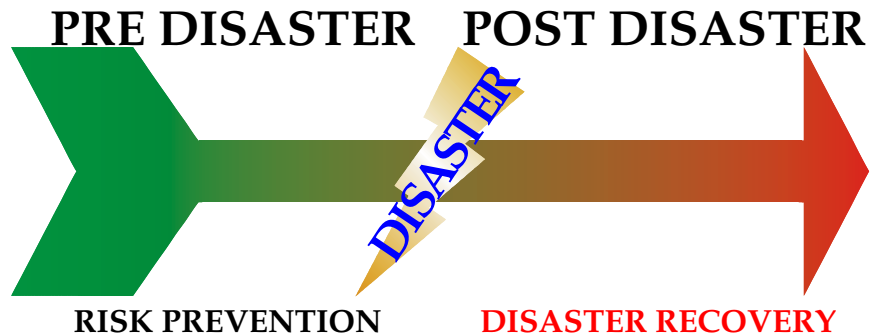
Mengurangi kemungkinan kejadian

Risk Mitigation →

Mengurangi konsekuensi kejadian

Budi Rahardjo

Disaster Timeline



Source: Lazuardi Nasution

Budi Rahardjo

Klasifikasi Keamanan

Menurut David Icove:

- Keamanan yang bersifat fisik (physical security).
- Keamanan yang berhubungan dengan orang (personel).
- Keamanan dari data dan media serta teknik komunikasi.
- Keamanan dalam operasi (policy & procedures)

Budi Rahardjo

Attacks on DRC

- Physical
 - Alam: kebakaran, banjir
 - Sengaja: Fasilitas dirusak, dibakar
 - Tidak sengaja: insiden (kopi tumpah)
- Personel
 - Key person meninggal

Budi Rahardjo

Attack on DRC

- Policy & Procedures
 - Seringkali tidak ada / tidak jelas
 - Siapa yang harus mengambil keputusan?
 - Langkah langkah apa yang harus diambil?
 - Belum pernah dilakukan drill / percobaan
 - Ada cost untuk melakukan itu

Budi Rahardjo

Investasi atau Cost



Budi Rahardjo

- Investasi di fire sprinkler akan terasa manfaatnya jika terjadi kebakaran.

Tahun 1882, sprinkler dianggap pemborosan.

- Apakah jika tidak ada apa-apa, maka dianggap sebagai pemborosan?
- ROSI = Return on Security Investment

Concluding Remarks

- Disaster Recovery perlu mendapat perhatian
- Masih banyak aspek yang perlu dibahas:
 - Technical
 - Non-technical (misal: Cost)

Budi Rahardjo