BAB 1

PENDAHULUAN

UNIKOM PERPUSTAKAAN UNIT PELAKSANA TEKNIS

1.1. Latar Belakang Masalah

Komputer merupakan investasi (asset) yang mempunyai nilai sangat tinggi, karena tidak hanya menyangkut perangkat keras (hardware) dan perangkat lunak sistem operasinya (software O/S) namun juga berkaitan dengan perangkat lunak aplikasi serta yang tidak kalah pentingnya adalah data dan sumber daya manusia, karena sulit untuk diukur/nilai dengan hitungan mata uang.

Bagi perusahaan-perusahaan yang menggunakan data komputer sebagai aset utama, bencana-bencana seperti : banjir, gempa bumi, kebakaran, ledakan bom maupun kerusuhan massa merupakan merupakan bencana yang sangat menakutkan.

Belum lagi sifat data komputer yang rentan yang bisa rusak hanya dengan hal-hal kecil, misalnya kerusakan akibat jaringan listrik atau akibat kesalahan operasional.

Suatu penelitian mengenai *Contingency Planning*, menunjukan bahwa sumber kerusakan tersebut paling banyak berasal dari :

1. kesalahan para pengguna atau operator.
2 Kesalahan (error) pada perangkat keras (hardware) maupun perangkat lunak (soft ware).
3 Kerusakan akibat jaringan listrik.
4 Bencana alam dan teroris.

Kehilangan atau kerusakan data bisa melumpuhkan atau mengacaukan kegiatan operasional perusahaan, termasuk kegiatan pelayanannya. Hal ini bisa berlangsung selama beberapa hari bahkan sampai beberapa minggu, sehingga nilai kerugian yang bisa berkembang dan berlipat ganda hanya dalam hitungan hari. Belum lagi kehilangan pelanggan karena ketidakpuasan dengan pelayanan yang terganggu, dan ini merupakan kerugian terbesar dari perusahaan.

Backup adalah nama lain yang biasa digunakan dalam dunia komputer untuk salinan atau copy data komputer.

Mengingat begitu rentannya data komputer terhadap kerusakan, *Backup* data diperlukan untuk keberlangsungan kegiatan–kegiatan yang menggandakan kerja komputer. Fungsi *backup* adalah sebagai cadangan data sehingga apabila terjadi kebakaran pada data dapat menjalankan kembali kegiatan operasi dan pelayanan dengan menggunakan backup data.

Backup data yang baik adalah data yang selalu diperbarui dan menyimpan data terakhir *(up-to-date)*. Oleh karena itu frekuensi pembuatan backup sangat tergantung pada jenis kegiatan yang dilakukan, kemudian hasil backup harus disimpan dalam ruang khusus yang tahan api.

Ruang seperti ini umumnya disebut *"vault"*, semacam lemari besi yang berdinding tebal dan dapat bertahan terhadap api selama beberapa jam.

Alternatif lain adalah copy back up data komputer disimpan dilokasi lain, yang biasa disebut lokasi *"off-site"*. Lokasi ini tentu harus dibangun dengan pertimbangan keselamatan dan ketahanan yang tidak kalah seriusnya dengan pusat datanya sendiri. Dengan demikian, jika gedung tempat pusat dat beroperasi musnah total karena

kebakaran atau bencana lainnya, *off-site* masih menyimpan backup data. Sehingga perusahaan masih dapat menjalankan kegiatannya karena data-data yang tersimpan tidak akan hilang/lenyap.

Masalahnya, keberlangsungan perusahaan tidaklah tergantung semata-mata pada keselamatan data yang terbaru, tapi lebih ditentukan pada seberapa cepat kegiatan operasional dapat kembali berjalan normal setelah terjadi bencana.

Apa yang terjadi pada sebuah perusahaan yang sistem komputernya tidak berfungsi selama beberapa hari karena pusat data mengalami kerusakan berat ?

Tentu saja hal ini harus dikaitkan dengan seberapa besar ketergantungan perusahaan pada komputer dan berapa besar kerugian yang akan dihadapi perusahaan tersebut, yang pada akhirnya menentukan kemampuan perusahaan itu untuk bertahan *(survive)*. Oleh karena itu, jika terjadi bencana, setiap perusahaan harus mengupayakan agar kegiatan usahanya dapat segera kembali berjalan dengan semaksimal mungkin dengan menggunakan sumber daya yang ada. Proses ini disebut **"Disaster Recovery".**

Kegiatan yang termasuk dalam proses ***Disaster Recovery*** adalah penggantian perangkat keras, penginstalasian perangkat lunak, restorasi data sampai dengan membentuk environment yang memungkinkan untuk menjalankan paling tidak kegiatan yang besifat kritikal. Proses ini akan jauh lebih mudah dan cepat dilakukan jika data dan aplikasi yang digunakan mempunyai backupnya.

Semua kegiatan ini secara rinci disusun di dalam apa yang disebut "***Disaster Recovery Plan".***

Ingatlah kata pepatah :" Sedia payung sebelum hujan "

1.2. Maksud dan Tujuan

Maksud dari laporan kerja praktek adalah sebagai salah satu ayarat mata kuliah kerja praktek pada jurusan Manajemen Informatika UNIKOM.

Adapaun tujuannya sebagai berikut:

- Menguraikan tentang hasil rancangan pengamanan komputer
- Dapat mengenal dalam pengunaan kompute secara global.

1.3. Metodologi Kerja Praktek

Metodologi kerja praktek yang digunakan dalam laporan ini penulis mencoba dengan tiga tehnik diantaranya:

1. Observasi Lapangan

   Mengumpulkan data tentang pengamanan komputer pada bagian tehnologi Informasi PT.PLN (Persero) Distribusi Jawa barat dan Banten.

2. Wawancara

   Untuk melengkapi dan memperjelas data untuk laporan ini maka penulis melakukan wawancara langsung kepada pihak-pihak yang bersangkutan

3. Literatur

   Untuk lebih memperjelas laporan ini, penulis mencoba mengambil dari buku-buku guna mendukung laporan akhir.

1.4. Lokasi dan Waktu

Masa pelaksanaan kerja praktek dilaksanakan tanggal 5 agustus 2003 sampai dengan 30 agustus yang bertempat tinggal di PT.PLN (Persero) di Jl. Cikapundung barat No.2 Bandung Tlp(022) 4230747.fax(022) 4207483.

1.5. Sistematika Penulisan

Sistematika pembahasan laporan ini menjelaskan urutan penulisan secara jelas, singkat, ringkas, dan sistematis.

BAB I : Pendahuluan

Bab ini berisikan latar belakang masalah, maksud tujuan, metodologi kerja praktek, lokasi dan waktu dan sistematika.

BAB II : Landasan Teori

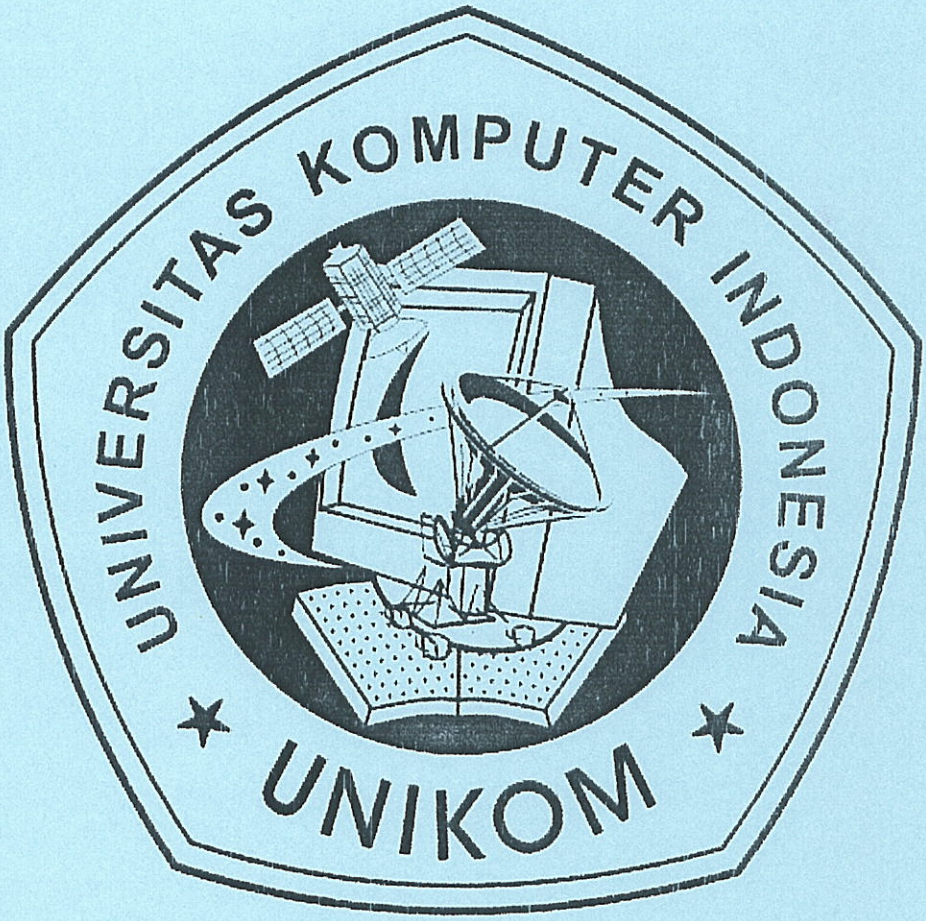
Bab ini berisikan mengenai landasan teori sejarah singkat perusahaan, struktur organisasi, deskripsi jabatan, pengamanan terhadap bahaya api, pengamanan terhadap bahaya banjir, penganmanan terhadap pencurian, dan pengamanan lain-lainnya.

BAB III : Pembahasan

Bab ini berisikan mengenai aspek kegiatan perusahaan, kegiatan dalam kerja praktek dan hasil kerja praktek, penganmanan masukan/input, proses komputer, keluaran/output dan pengamanan sistem.

BAB IV : Kesimpulan Dan Saran

Bab ini berisikan kesimpulan secara garis besar, dari hasil analisa penelitian tentang komputer dan sistem pengamanan serta pencegahannya. Dan saran untuk perusahaan tempat penulis melaksanakan kerja praktek.


UNIVERSITAS KOMPUTER INDONESIA
UNIKOM