PEMANFAATAN CLOUD STORAGE DALAM PERENCANAAN SUATU PEMULIHAN BENCANA TEKNOLOGI INFORMASI *(IT DISASTER RECOVERY PLANNING)*

Asril Basry[1], **Essy Malays Sari**[2]

[1)] *Sistem Informasi Fakultas Teknik UPI YAI Jakarta*
[2)] *Teknik Informatika Fakultas Teknik UPI YAI Jakarta*
Jl Salemba Raya Jakarta Pusat
Email : basrya@hotmail.com[1)], malays@yahoo.com[2)]

Abstrak

Perencanaan suatu pemulihan adanya bencana teknologi informasi (IT Disaster Recovery Planning), adapun bencana yang dimaksud seperti terjadi kebakaran , bencana alam , perang dll sehingga dapat menyebabkan kerusakan pada infrastruktur teknologi informasi dalam hal ini adalah media penyimpanan data (data storage). Salah satu strategi yang dilakukan suatu perusahaan adalah membuat merencanakan pemulihan bencana dengan memanfaatkan teknologi cloud storange. Adapun cloud storage merupakan salah satu bagian dari cloud computing yang dilakukan oleh pihak penyedia layanan internet atau internet provider. Perusahaan dapat menyalin atau back data kedalam cloud storage dengan diupdate atau dimutahkirkan secara berkala sehingga jika suatu kondisi terjadi bencana yang menyebabkan tidak berfungsinya fasilitas dan infrasturktur teknologi informasi dalam hal ini media penyimpanan data (data storage) , maka perusahan dapat melanjutkan pengolahan data dengan menggunakan data yang disimpan dalam cloud storage, adapun dalam cloud storage tetap menjamin terhadap keamanan dan kerahasian data perusahaan. Didalam tulisan ini berisi penjelasan mengenai pemulihan pasca bencana TI (disaster recovery IT) dimana agar perlu diadakan perencanaan terhadap pemulihan bencana teknologi informasi dengan memanfaatkan teknologi cloud storage.

Kata kunci: *Perencanaan, pemulihan , bencana, cloud, Storage.*

1. Pendahuluan

1.1 Latar Belakang

Dalam suatu jaringan komputer di suatu perusahaan terutama di perusahaan besar dan multi nasional , perencanaan suatu pemulihan adanya bencana (Disaster recovery) merupakan sesuatu strategi yang sangat penting dalam menghadapi kejadian bencana yang tidak diharapkan terhadap infrastruktur teknologi informasi. Apabila hal ini tidak dilakukan maka perusahaan akan mendapat kesulitan untuk melanjutkan proses pengolahan data dan bisa memungkinkan dapat dapat mengakibatkan bisnis di perusahaan akan terhenti (business interruption). Dalam suatu incident atau kejadian dimana suatu kebakaran melanda sebuah server-room dimana berada didalamnya seluruh server dan menghancurkan semua yang ada didalamnya termasuk semua peralatan server dan infrastruktur pendukungnya seperti router, Switches, jaringan kabel termasuk media penyimpanan data atau data storage dan apapun – semuanya tak tersisa sama sekali , sehingga perlu diadakan pemulihan terhadap infrastruktur yang tidak berfungsi tadi.

Dalam tulisan ini penulis menggunakan model penulisan overview dengan beberikan pandangan , penjelasan dan melakukan peninjauan terhadap aspek pemulihan bencana terhadap Teknologi Informasi. Pemulihan Bencana adalah data dan informasi, sebagaimana telah disebutkan sebelumnya sangat penting untuk menjaga kekonsistenan dari data dan informasi bagi perusahaan. Kebutuhan ini dapat diakodomasi dengan menggunakan teknologi replikasi data. Replikasi data adalah sebuah proses yang mengkopi isi data ke suatu lokasi *remote* baik yang berlangsung secara kontinu ataupun pada interval tertentu. Replikasi data akan menyediakan hasil kopi data yang lengkap untuk tujuan Pemulihan Bencana. Lokasi remote biasanya merupakan penyimpanan secondary data .

Penelitian sebelumnya adalah yang dilakukan terhadap pemulihan bencana call center pada industri perbankan [9] dan Studi kelayakan DRP pada infrastruktur jaringan Komputer [10]. Adapun perbedaan penelitian yang dilakukan penulis terhadap penelitian sebelumnya adalah untuk melakukan replika terhadap data dengan melakukan penyimpanan data (storage) di cloud storage yang dimiliki oleh sebuah provider yang menyediakan layanan cloud computing untuk melakukan antisipasi jika terjadi suatu bencana terhadap teknologi informasi ,dimana kedua penelitian sebelumnya diatas lebih membahas pada aspek penyimpan data dengan konsep remote storage dan berada diluar perusahaan [9] serta pemulihan bencana terhadap infrastruktur jaringan [10]

Data merupakan suatu yang sangat penting sehingga untuk pemulihan agar bisa beroperasinya pengolahan

data dan diakses oleh pemakai atau user bisa menggunakan teknologi cloud storage dimana data perusahan yang disimpan di suatu provider penyedia layanan cloud storage dan dapat dilakukan restore sehingga proses pengolahan data dapat dilanjutkan seperti sebelum terjadinya bencana.

1.2 Perumusan Masalah

Perusahaan sudah seharusnya mengelola infrastruktur sistem dan melindunginya terhadap segala macam bentuk ancaman dan bahaya yang mengganggu jalannya pengoperasian dan pengolahan data serta juga mengelola sistem perencanaan pemulihan bencana atau disaster recovery planning dan business continuity planning setelah pasca bencana terhadap segala macam bentuk kerusakan dan kehilangan data dalam hal adanya bencana.

Dalam membuat perencanaan pemulihan bencana terhadap infrastruktur teknologi informasi terutama kerusakan terhadap penyimpanan data (data storage) dibutuhkan suatu teknologi yang dapat mengatasi jika kerusakan terhadap penyimpanan data dan melakukan pemulihan segera (data recovery) sehingga proses pengolahan data tidak terhenti.

1.3 Tujuan

Adapun tujuan dari rencana pemulihan bencana atau disaster recovery planning diutamakan untuk mengatur dan mementukan suatu cara yang terstruktur untuk membuat keputusan jika suatu kejadian atau incident yang terjadi mengganggu jalannya proses pengolahan data, selain itu tujuan disaster recovery adalah untuk mengurangi ketidaktahuan dari perusahaan dan meningkatkan kemampuan perusahaan untuk sehubungan dengan bencana tersebut. Sesungguhnya, ketika suatu peristiwa yang mengganggu terjadi, perusahaan tidak akan mempunyai kemampuan untuk menciptakan dan melaksanakan suatu rencana pemulihan dengan segera. Oleh karena itu, jumlah perencanaan dan pengujian yang telah dilakukan sebelumnya akan menentukan kemampuan perusahaan tersebut dalam menangani pemulihan bencana terhadap teknologi informasi terutama penyimpanan data.

Tujuan tujuan dari rencana pemulihan bencana meliputi:

1. Melakukan proteksi dan perlindungan di perusahaan dari kegagalan penyediaan layanan jasa Komputer.
2. Memperkecil risiko keterlambatan suatu perusahaan dalam pegolahan data
3. Menjamin pengoperasian pegolahan data secara normal pasca terjadinya bencana
4. Menggunakan suatu teknologi penyimpanan data online (cloud storage) diluar sistem penyimpanan data perusahaan.

1.4 Metodologi

Metode yang dipilih adalan melakukan pengamatan atau observasi terhadap perusahan atau organisasi yang ada di Indonesia. Selain itu akan mengambil dari beberapa literatur dan melakukan studi kepustakaan.

1.5 Landasan Teori

Langkah langkah yang dilakukan dalam melakukan perencanaan pemulihan bencana [2] :

1. Sumber dari bencana
2. Analisa dampak terhadap bisnis
3. Backup and Strategi pemulihan
4. Recovery

Penggunaan cloud computing dapat menyediakan sendiri sumber daya komputasi yang dibutuhkan seperti misalnya virtual machine atau cloud storage sesuai dengan kebutuhan perusahaan tanpa harus ada interaksi dari pihak provider atau penyedia jasa cloud computing [3]. Cloud Storage saat ini telah menjadi salah satu aplikasi yang banyak digunakan untuk menyimpan data secara aman dan berbayar. Keunggulan dari penggunaan cloud storage ini adalah perusahaan bisa mengakses data penting anda dimana saja dan kapan saja saat kita bisa terhubung di internet.

2. Pembahasan

Mengirim data backup secara berkala ke tempat penyimpanan diluar ruang server disatu lokasi perusahaan (offsite storage) merupakan hal yang sering dilakukan oleh suatu perusahaan. Dengan tersedianya mesin server di tempat terpisah (dari server room yang terbakar atau rusak) maka bisa melakukan restore data ke mesin atau infrastruktur cadangan agar memungkinkan pemakai bisa mulai melanjutkan pekerjaannya dalam batas minimum agar bisa operasional saja. Proses inilah yang disebut bagian dari Disaster Recovery (DR). Saat terjadi bencana atau disaster kerusakan tidak hanya melanda ruang server tetapi juga tempat penyimpanan back-up data (offstorage)

2.1 Strategi Pencegahan dan mitigasi risiko

Dalam pertencanaan pemulihan bencana atau disaster recovery planning eharusnya juga mencakup strategi pencegahan yang meliputi metoda-metoda yang harus diambil untuk menghindari potensi terjadinya suatu bencana terhadap infrastruktur teknologi informasi.

Selain itu dalam membuat perencanaan pemulihan bencana juga harus mengenali sumber sumber dari bencana seperti terlihat pada Tabel 2.1 :

Tabel 2.1 Sumber – sumber bencana

Sources of Disaster

Nature / Technology / Organization / People	
Accidental	**Malicious**
Fire / Lightning / Smoke	
Earthquake / Tornado / Flood	
Building Collapse	
Strikes / Industrial Actions	
War / Invasion	
Hardware / Software Problems	
Loss of plant / systems / services / data "availability"	

Saad Haj Bakry, *PhD, CEng, FIEE*

Berdasarkan dari sumber sumber diatas dapat dilakukan mitigasi dari resiko dan biasanya di-implementasikan sepanjang temuan potensi resiko. Berikut adalah contoh-contoh strategi pencegahan:

1. Backup dapat dilakukan dengan harian, mingguan, dan bulanan dan data disimpan offsite. Alasan disimpan terpisah atau offsite adalah kalau disimpan ditempat / di gedung yang sama, jika terjadi bencana seperti contohnya kebakaran , banjir , perang maka perusahaan kehilangan semuanya tidak hanya software dan aplikasi berikut juga dengan infrastruktur lainnya termasuk penyimpanan data atau data storage.
2. Memperbaiki dan mengelola dengan baik keamanan data dan infrastruktur termasuk perlindungan terhadap firewall System yang bisa merupakan ancaman dari pihak luar sistem atau internet.

2.2 Risiko Sistem Data

Risiko sistem data berhubungan dengan penggunaan infrastruktur secara bersamaan seperti networks , file servers dan perangkat lunak aplikasi yang akan berdampak pada pengoperasian dan penggunaan komputer di perusahaan atau organisasi , kerusakan pada infrastruktur komputer termasuk penyimpanan data membutuhkan waktu yang lama dan tentunya dengan biaya yang cukup besar, untuk itu perlu dibuatkan kategori dari risiko sistem data [1] sebagai berikut :

- Data communication network
- Telecommunication systems and network
- Shared servers
- Virus
- Data backup/storage systems
- Software applications and bugs

2.3 Menentukan efek dan dampak dari bencana

Saat kita telah melakukan analisa terhadap risiko bencana dan selanjutnya menentukan efek dari bencana dan dampaknya terhadap pengoperasian dan penggunaan komputer di perusahaan atau organisasi, misalnya seperti gambar 2.2 dimana terjadi bencana gempa bumi atau earthquake dapat mengakibatkan kerusakan dari sistem data termasuk kerusakan media penyimpanan data (data storage) dan merupakan suatu yang sangat kritis apabila data sudah rusak dan tidak dapat digunakan sehingga dapat memungkinkan pengolahan data menjadi berhenti serta bukan tidak mungkin bisnis diperusahaan menjadi terhenti (bisnis interruption)

Gamabr 2.2 Dampak bencana Gempa Bumi

2.3 Prosedur Pemulihan (Recovery Procedure)

Perencanaan pemulihan bencana sebaiknya memiliki rincian prosedur untuk melakukan restore system atau system components sehingga pengoperasian teknologi informasi di perusahaan dapat normal kembali. proses untuk melakukan pemulihan bencana terhadap pelayanan teknologi informasi sebagai berikut

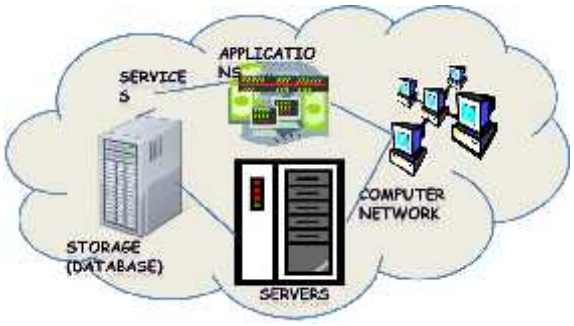
1. Memberikan notifikasi dan pemberitahuan tentang Kerusakan kepada pemakai
2. Mendapatkan tempat bekerja dan infrastrukturnya
3. Mendapatkan dan install H/W beserta komponennya
4. Mendapatkan dan load backup data
5. Restore sistem operasi dan software aplikasi
6. Restore sistem data dan load backup data
7 Melakukan test system functionality termasuk security controls
8. Melakukan koneksi sistem ke network atau jaringan

luar lainnya

Untuk menghindari masalah saat situasi darurat pasca bencana diharapkan dibuatkan dokumentasi dari prosedur ini dengan format yang sederhana dan dilengkapi dengan langkah lahkah untuk menjalanlan prosedur pemulihan pencana teknologi informasi

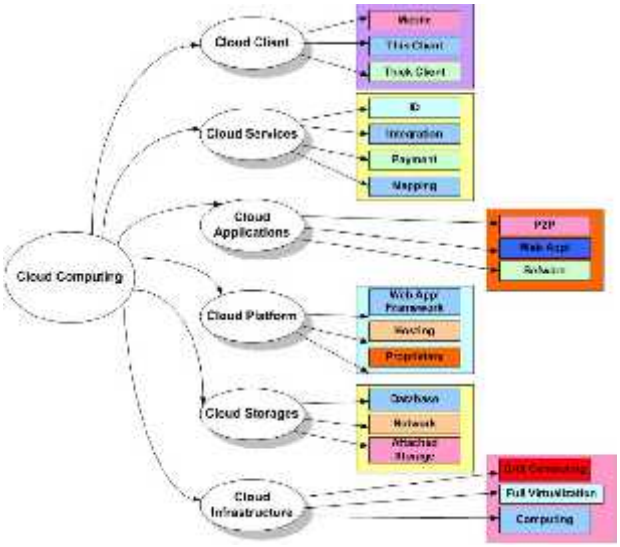
2.4 Cloud Computing

Cloud computing atau komputasi awan dimana data data layanan berada pada sumber daya yang digunakan bersama (shared resources) dalam suatu pusat data dengan menggunakan internet. Komputasi awan merupakan teknologi yang memanfaatkan layanan menggunakan pusat server yang disediakan oleh suatu provider dan bersifat virtual dengan tujuan pemeliharaan data Komputasi awan atau cloud computing dengan menggunakan suatu provider yang dapat memberikan pelayanan terhadap penggunaan perangkat lunak (software) , penyimpanan data (storage) , Jaringan (network) serta komputasi data menggunakan server termasuk penggunaan Web [3]. (seperti yang terlihat Gambar 2.3).



Gambar 2.3 Konfigurasi Cloud Computing

Salah satu layanan yang diberikan oleh cloud computing adalah cloud storage [3] (Gambar 2.4). Cloud storage atau dikenal dalam bahasa baku penyimpanan awan adalah sebuah layanan penyimpanan data online yang terintegrasi dan tersinkronisasi melalui internet dan dapat di akses dengan menggunakan berbagai platform (OSX, iOS, Windows, WindowsMobile, Android, Linux, Blackberry, Symbian dan lain-lain). Komputasi awan menjadi sangat dikenal di dunia IT beberapa tahun belakangan ini beberapa pemain besar dunia IT lainnya seperti: Cisco, Oracle , Google, Microsoft hingga Amazon turut andil memperkenalkan produk terbaru mereka di dalam peta persaingan komputasi awan.



Gambar 2.4 Cloud Storage

Penulis mengusulkan untuk melakukan back up data menggunakan cloud storage dimana menyalin data atau back up data dapat dilakukan dengan frekwensi harian , mingguan atau bulanan. Dimana jika terjadi suatu bencana terhadap teknologi informasi makan proses pemulihannya atau recovery dapat menggunakan data yang disimpan pada cloud storage,

3. Kesimpulan dan Saran.

Data merupakan suatu asset yang sangat penting diperusahaan sudah seharusnya perusahaan memberikan perlindungan sangat baik serta paling utama adalah perusahaan dapat melakukan pemulilhan kembali operasional pengolahan data tanpa kehilangan data berharga jika terjadi suatu bencana (disaster). Untuk itulah perusahaan harus mengembangkan sistem perencanaan pemulihan bencana atau disaster recovery planning di suatu perusahaan

Disaster recovery planning memberikan suatu kerangka kerja untuk membuat suatu penyelamatan / recovery infrastructure IT anda dari segala macam bencana baik yang berskala kecil maupun besar. Suatu disaster recovery planning memberikan daftar yang sudah dibuat dan koordinasi dari langkah-langkah yang perlu dilakukan untuk meminimalkan akibat dari suatu bencana dan membantu perusahaan dalam mempercepat pemulihan sistem.

Dalam upaya penangan pemulihan bencana , penulis mengusulkan untuk menggunakan teknologi cloud storage dimana data –data disalin atau back up menggunakan cloud storage yang merupakan salah satu pelayanan cloud computing yang disediakan oleh internet provider , sehingga jika terjadi bencana data tersebut bisa dilakukan proses restore sehingga pengolahan data dapat dilanjutkan.

Penulis memberikan beberapa saran antara lain :

1. Mengembangkan dan melakukan implementasi terhadap standard ISO 24.782 dalam pemulihan bencana teknologi informasi
2. Melakukan penelitian lebih lanjut terhadap perencanaan kelanjutan bisnis (Business Continuity Plan) pasca terjadinya bencana terhadap teknologi informasi.
3. Melakukan analisa lebih lanjut terhadap kemampuan provider atau penyedia layanan outsourcing Teknologi Informasi (ICT).

Daftar Pustaka

[1] L.A. Worbel ,"*Disaster Recovery Planning for Telecommunications, ," :* Artech House (US), 1990.
[2] Saad Haj Bakry, *PhD, CEng, FIEE*, "Contigency and recovery Planning," *Presentation in network security*, pp. 758-765, Sept. 3-7, 2006.
[3] Rittinghouse, JW , & Ransome JF, 2010, "*Cloud computing Implementation , Management & Security*," New York : Taylor and Francis Group.
[4] Neal Cross and Shelly Brown, "Disaster Recovery Plan" *in Seminar Southwest Baptist University, Bolivar, Missouri*, 2008.
[5] Mardecia Bell and Ann Harris ,"Disaster Recovery and Business Continuity Plan", *in Seminar NC StateUniversity* 10-11, March ,2005.
[6] Indra Riawan,"Rencana Pemulihan dari Bencana (Disaster Recovery Plan (DRP)", *Seminar IT* 10-11, Juni ,2010
[7] Bank Central Asia,"Teknologi Informasi", *Laporan Tahunan inftrastruktur IT BCA 2011.*
[8] Sertifikasi Manajemen Mutu,"ISO 24.762 Standard untuk pemulihan bencana", *ISO Panduan Pemulihan Bencana ,September 2012*
[9] Dolly Irham ,"Kajian Disaster Recovery Call Center Pada Industri Perbankan", *Tesis MTI UI* , 2008.
[10] Rachmaningrum, Nilla dan Falahah,"Studi Kelayakan Disaster Recovery Plan pada infrastruktur jaringan computer (Studi Kasus Jaringan Komputer Universitas Widtyatama)", *Seminar nasional informatika* , 2011.

Biodata Penulis

Nama Lengkap Penulis Pertama,memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Manajemen Informatika STI & K Jakarta, lulus tahun 1996. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Manajemen Teknik Informatika Universitas Indonesia Jakarta, lulus tahun 1999. Saat ini menjadi Dosen di Fakultas Teknik Universitas Persada Indonesia YAI Jakarta.

Nama Lengkap Penulis Kedua,memperoleh gelar Sarjana Komputer (Ir), Jurusan Teknik Komputer Universitas Gunadarma Jakarta, lulus tahun 1992. Memperoleh gelar Magister Manajemen Sistem Informasi (MMSI) Program Pasca Sarjana Magister Teknik Informatika Universitas Gunadarma Jakarta, lulus tahun 2007. Saat ini menjadi Dosen di Fakultas Teknik Universitas Persada Indonesia YAI Jakarta.

ISSN : 2302-3805