Tugas Kelompok

Sistem Informasi Manajemen (SIM)

Dosen : Prof. Dr. Ir. Kudang B. Seminar, MSc

DATA BASE & SECURITY
SISTEM INFORMASI MANAJEMEN

www.belibarang.com

Kelompok III (Lemon)

Abrori	P056100012.35E
Agus Prihanto	P056100042.35E
Elfa Astrid Triyani	P056100172.35E
Indra Harimurti SP.	P056100212.35E
Inggrid Clarissa W.	P056100232.35E
Rurin Wahyu L.	P056100362.35E

PROGRAM PASCASARJANA MANAJEMEN DAN BISNIS
INSTITUT PERTANIAN BOGOR
2011

DAFTAR ISI

DAFTAR TABEL

I. PENDAHULUAN

1.1. Latar Belakang

Saat ini, penggunaan teknologi informasi (TI) di perusahaan semakin meningkat. Tidak hanya untuk proses operasional sehari-hari, tetapi juga dalam proses pengambilan keputusan. Bahkan, di beberapa sektor industri seperti perbankan dan keuangan, ketergantungan pada TI sangat besar.

Dalam beberapa tahun terakhir ini juga Electronic Commerce mulai mendapat perhatian besar di Indonesia. Bahkan sudah ada banyak implementasi dari e-commerce. Namun masih ada kendala dalam penerimaan e-commerce ini yaitu adanya masalah akan kepercayaan dan keamanan (security).

Masalah utama yang dihadapi adalah belum adanya pemahaman dan kepedulian (awareness) akan masalah keamanan. Memang dapat dimengerti bahwa penerapan e-commerce di Indonesia ini masih pada tahap awal sehingga fokus utamanya bukan pada masalah keamanan akan tetapi pada keberadaannya dan pengelolaannya dahulu. Tanpa penerapan sistem pengamanan pada sistem e-commerce, masalah akan timbul di kemudian hari yaitu menurunnya kepercayaan customer dan akhirnya ditinggalkan karena customer tidak berani menggunakan fasilitas tersebut.

Data base customer juga merupakan asset yang sangat penting bagi perusahaan, data base yang dimiliki merupakan sarana potensial untuk berjualan atau berpromosi, sehingga produk dapat dikenal dan dibeli.

Aspek *integrity* (integritas) terkait dengan keutuhan data. Aspek ini menjamin bahwa data tidak boleh diubah (*tampered, altered, modifed*) tanpa ijin dari yang berhak. Acaman terhadap aspek integritas dilakukan dengan melalui penerobosan akses, pemalsuan (spoofing), virus yang mengubah atau menghapus data, dan *man in the middle attack* (yaitu penyerangan dengan memasukkan diri di tengah-tengah pengiriman data). Proteksi terhadap serangan ini dapat dilakukan dengan menggunakan *digital signature*, *digital certificate, message authentication code*, *hash function,* dan *checksum*. Pada prinsipnya mekanisme proteksi tersebut membuat kode sehingga perubahan satu bit pun akan mengubah kode.

1.2. Tujuan

Tujuan penulisan makalah ini adalah:

1. Mengetahui dan membuat kebutuhan database Perusahaan menggunakan *backward analysis* dari proses bisnis tersebut.
2. Mengetahui keterkaitan antar data dalam *data base* tersebut.
3. Mengidentifikasi berbagai kemungkinan kerawanan data yang bisa terjadi dari proses bisnis di tersebut.
4. Membuat perencanaan pengamanan data secara elektronik, fisik, maupun prosedural dari proses bisnis tersebut.

II. TINJAUAN PUSTAKA

2.1. Sistem Informasi Manajemen

O'brien menjelaskan bahwa sistem informasi merupakan kombinasi teratur apapun dari manusia, hardware, software, jaringan komunikasi, dan sumber daya data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Sistem informasi manajemen terdiri dari tiga kata yang mempunyai pengertian masing-masing,

a. Sistem yaitu suatu susunan yang teratur dari kegiatan-kegiatan yang saling berkaitan dan susunan prosedur-prosedur yang saling berhubungan, yang melaksanakan kegiatan-kegiatan utamanya.
b. Informasi adalah data yang telah diproses/diolah sehingga memiliki arti satu manfaat yang berguna.
c. Sedangakan manajemen sebagai proses adalah kegiatan yang dilakukan untuk menyelesaikan suatu pekerjaan secara bersama-sama atau melibatkan orang lain demi mencapai tujuan yang sama.

Dari definisi diatas maka dapat disimpulkan bahwa pengertian sistem informasi manajemen adalah jaringan prosedur pengolahan data yang dikembangkan dalam suatu sistem (terintegrasi) dengan maksud memberikan informasi (yang bersifat intern dan ekstern) kepada manajemen sebagai dasar pengambilan keputusan.

Sedangkan menurut Mutia Ismail sistem informasi manajemen yaitu: serangkaian sub-sistem informasi yang menyeluruh dan terkoordinasi yang secara rasional mampu mentransformasikan data sehingga menjadi informasi dengan berbagai cara guna meningkatkan produktivitas yang sesuai dengan gaya dan sifat manajer.

2.2. DBMS *(Data Base Management System)*

Data merupakan suatu hal yang sangat penting untuk suatu organisasi atau persahaan. Data adalah catatan atas kumpulan fakta. Data merupakan bentuk jamak dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan".

Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Pernyataan ini adalah hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata, atau citra.

Dalam keilmuan (ilmiah), fakta dikumpulkan untuk menjadi data. Data kemudian diolah sehingga dapat diutarakan secara jelas dan tepat sehingga dapat dimengerti oleh orang lain yang tidak langsung mengalaminya sendiri, hal ini dinamakan deskripsi. Pemilahan banyak data sesuai dengan persamaan atau perbedaan yang dikandungnya dinamakan klasifikasi.

Menurut O'Brien (2005) DBMS adalah *software* utama dalam pendekatan manajemen database, karena software tersebut mengendalikan pembuatan, pemeliharaan,dan penggunaan database organisasi dan pemakai terakhir.

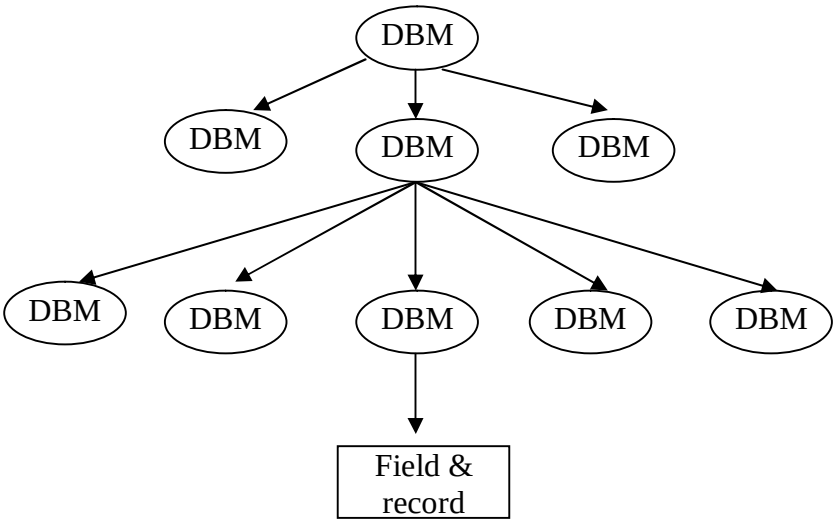
Menurut Oetomo (2002) database merupakan komponen terpenting dalam pembangunan SI. Karena menjadi tempat menampung dan mengorganisasikan seluruh data yang ada dalam sistem, sehingga dapat diekplorasi untuk menyusun informasi-informasi dalam berbagai bentuk.

Menurut Date, sistem Basis Data adalah sistem terkompeterisasi yang tujuan utamanya adalah memelihara informasi dan membuat informasi tersebut tersedia saat dibutuhkan. Sedangkan Manajemen Sistem Basis Data *(database Management System* - DBMS) adalah perangkat lunak yang didesain untuk membantu dalam hal pemeliharaan dan utilitas kumpulan data dalam jumlah besar. DBMS dapat menjadi alternatif penggunaan secara khusus untuk aplikasi, semisal penyimpanan data dalam fiel dan menulis kode aplikasi yang spesifik untuk pengaturannya.

Pengembangan bidang sistem basis data mengalami kemajuan dari tahun-ketahun, sehingga DBMS mengalami perkembangan dalam aplikasinya, terdapat pengembangan untuk sistem khusus/spesial yang dikembangkan oleh beberapa vendor untuk membuat *data warehouse*, mengkonsolidasi data dari beberapa basis data. Penomena yang paling menarik adalah adanya enterprise resource planning (ERP) dan management resource planning (MRP) yang menambahkan substasial layer dari fitur berorientasi pada aplikasi.

Beberapa software atau perangkat lunak DBMS yang sering digunakan dalam aplikasi program antara lain DB2, Microsoft SQL Server, Oracle, Sybase,

Interbase, Teradata, Firebird, MySQL, dan PostgreSQL. Dalam konsep database, urutan atau hierarki database sangatlah penting. Urutan atau hierarki database digambarkan dalam gambar sebagai berikut:



Gambar 1. Urutan atau Hirarki *Data Base*

(Sumber : Asep Herman Suyanto, 2004)

a. Komponen Utama DBMS

Komponen utama DBMS dapat dibagi menjadi 4 macam yaitu Perangkat Keras, Perangkat Lunak, Data dan Pengguna

b. Keuntungan Penggunaan DBMS

1. Kebebasan data dan akses yang efisien
2. Mereduksi waktu pengembangan aplikasi
3. Integritas dan keamanan data
4. Administrasi keseragaman data
5. Akses bersamaan dan perbaikan dari terjadinya crashes (tabrakan dari proses serentak)

Menurut O'Brien ada tiga fungsi dasar dari sistem manajemen database adalah

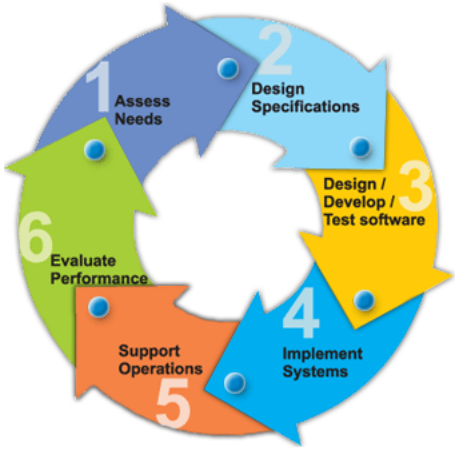
- Untuk membuat database baru dan aplikasi database.
- Memelihara kualitas data dalam database organisasi.

- Menggunakan database organisasi untuk memberikan informasi yang dibutuhkan oleh para pemakai akhir.

Para pemakai akhir dapat menggunakan DBMS untuk menanyakan informasi dari database dengan menggunakan fitur permintaan (*query*) atau pembuat laporan (*report generator*).

Dalam model klien/server, sebuah aplikasi dibagi menjadi dua bagian yang terpisah, tapi masih merupakan sebuah kesatuan yakni komponen klien dan komponen server. Komponen klien juga sering disebut sebagai *front-end*, sementara komponen server disebut sebagai *back-end*. Komponen klien dari aplikasi tersebut dijalankan dalam sebuah workstation dan menerima masukan data dari pengguna. Komponen klien tersebut akan menyiapkan data yang dimasukkan oleh pengguna dengan menggunakan teknologi pemrosesan tertentu dan mengirimkannya kepada komponen server yang dijalankan di atas mesin server, umumnya dalam bentuk*request* terhadap beberapa layanan yang dimiliki oleh server. Dalam sistem secara umum server proses pada DBMS, komponen server akan menerima request dari klien, dan langsung memprosesnya dan mengembalikan hasil pemrosesan tersebut kepada klien.

Analisis kebutuhan database pada kasus ini menggunakan metodologi *backward requirement analysis*, yaitu menganalisis kebutuhan database dengan penurunan kebutuhan dari fungsi manajemen, tujuan manajemen dan informasi yang dibutuhkan. Fungsi manajemen yang dapat diidentifikasi dari kasus dibagi menjadi 4 fungsi yaitu perencanaan (*planning*), pengarahan (*directing*), aksi (*acting*) dan pengawasan (*monitoring*). Untuk menganalisa dan mendapatkan daftar kebutuhan pengguna (user) terhadap sistem yang akan dibangun juga bukan merupakan pekerjaan yang mudah. Mengingat beragamnya pola pikir dan cara pandang pengguna terhadap pengembangan *software* sering membuat proses analisa kebutuhan pengguna *(requirement gathering)* terhambat. Gambra berikut memberikan gambaran tips atau langkah sederhana yang dapat dilakukan untuk menganalisa kebutuhan pengguna terhadap sistem yang akan dibuat.



Gambar 2. Siklus Analisis Data

Sumber : (http://www.acmatim.net, diakses pada 8 Juni 2010)

2.3. *Security Management* Data

Dengan pesatnya peningkatan akses Internet, seseorang dapat berpikir bahwa halangan terbesar dalam *e-commerce* adalah tingkat transmisi informasi (bandwidth), akan tetapi bukan hal itu. Masalah utamanya adalah keamanan. Sebagian dari masalah itu adalah internet dikembangkan untuk dapat dioperasikan dari mana saja, bukan untuk ketahanan.

Ancaman banyak terjadi pada internet, dan ancaman tersebut sangat signifikan atas keamanan dari sistem informasi dalam bisnis. Maka perlu dibuat sistem keamanan yang bertanggung jawab atas keamanan, kualitas, dan kinerja dari sistem informasi bisnis dalam unit bisnisnya. Seperti aset penting bisnis lainnya, hardware, software, jaringan, dan sumber daya data perlu dilindungi oleh berbagai alat keamanan untuk memastikan kualitas dan keamanannya.

Menurut O'brien (2005) tujuan dari manajemen keamanan adalah untuk akurasi, integritas, dan keamanan proses serta sumber daya semua sistem informasi. Jadi, manajemen keamanan yang efektif dapat meminimalkan kesalahan, penipuan, dan kerugian dalam sistem informasi yang saling menghubungkan perusahaan saat ini dengan pelanggan, pemasok, dan *stakeholder* lainnya.

Keamanan dari perusahaan saat ini menjadi tantangan manajemen yang terbesar. Banyak perusahaan masih dalam proses untuk dapat terhubung penuh

dengan *Web* dan *Internet* untuk *e-commerce*, dan merekayasa ulang proses bisnis internalnya. Ada beberapa pertahanan keamanan yang penting, diantaranya :

a. Enkripsi

Sangat penting untuk melindungi data dan sumber daya jaringan komputer lainnya terutama di Internet, intranet dan ekstranet. Enkripsi melibatkan penggunaan algoritma matematika khusus, atau kunci, untuk mengubah data digital ke dalam kode acak sebelum ditransmisikan, serta untuk melakukan dekode data tersebut ketika mereka diterima. Program enkripsi dijual sebagai produk terpisah atau dimasukkan ke dalam software lain yang digunakan untuk proses ekripsi.

b. Firewall

Sistem *Firewall* sebuah jaringan dapat merupakan prosesor komunikasi, biasanya sebuah router, atau server khusus, bersama dengan *software firewall*. *Firewall* berfungsi sebagai "penjaga gerbang" sistem yang melindungi intranet perusahaan dan jaringan lain perusahaan dari penerobosan, dengan menyediakan saringan dan *point transfer* yang aman untuk akses ke dan dari internet serta jaringan lainnya.

Firewall dapat mendeteksi akses yang masuk, tetapi tidak benar-benar dapat mencegah secara keseluruhan akses tidak sah *(hacking)* ke dalam jaringan komputer. Dalam beberapa kasus, *firewall* dapat mengizinkan akses hanya dari lokasi yang dipercaya di Internet ke komputer tertentu di dalam *firewall*. Atau, *firewall* dapat hanya mengizinkan para pemakai untuk membaca e-mail dari lokasi jarak jauh tetapi tidak dapat menjalankan program tertentu.

Untuk melindungi sistem dan jaringan dalam bisnis, banyak sekali alat atau pengaman yang digunakan. Hal ini meliputi alat *hardware* dan *software* seperti komputer yang bertoleransi pada kegagalan dan pemonitoran keamanan, serta kebijakan dan prosedur keamanan seperti *password* dan file cadangan. Ada berbagai macam cara yang digunakan untuk sebagai alat pengamanan, yaitu :

1. Kode keamanan

Merupakan sistem password bertingkat yang digunakan untuk manajemen keamanan. Di dalam beberapa sistem, *password* untuk membaca isi file

berbeda dari yang diminta untuk menulis ke sebuah file (mengubah isinya). Fitur ini menambahkan tingkat perlindungan untuk sumber daya data yang disimpan.

2. **Pembuatan cadangan file**

   Pembuatan cadangan file (*backup file)* yang diduplikasi berbagai file data atau program, adalah alat keamanan lainnya. file juga dapat dilindungi dengan alat file *retention* yang melibatkan penyimpanan berbagai kopi file dari periode sebelumnya.

3. **Pemonitor Keamanan**

   Keamanan suatu jaringan dapat disediakan oleh paket software sistem khusus yang disebut sebagai pemonitor keamanan sistem *(system security monitor)*. Pemonitor keamanan sistem adalah program yang memonitor penggunaan sistem komputer dan jaringan serta melindungi mereka dari penggunaan tidak sah, penipuan, dan kehancuran.

4. **Keamanan Biometris (*biometric system)***

   Adalah bidang keamanan komputer yang mengalami pertumbuhan pesat. Ini adalah alat keamanan yang disediakan oleh peralatan komputer, yang mengukur ciri khas fisik yang membedakan setiap individu. Hal ini meliputi verifikasi suara, sidik jari, geometri tangan, dinamika tanda tangan, analisis pendekatan tombol, pemindai retina mata, pengenal wajah, serta analisis pola geometrik.

5. **Pengendalian Kegagalan Komputer**

   Adalah sistem pengendalian yang digunakan untuk meminimalkan pengaruh kegagalan, baik itu melalui sistem komputer ataupun diakibatkan oleh matinya listrik, serta tidak berfungsinya sirkuit elektronik. Untuk meminimalkan terjadinya kerusakan, maka diperlukan sistem komputer cadangan untuk meminimalkan terjadinya kehilangan data.

6. **Sistem Teloransi Kegagalan**

   Yaitu sistem yang didukung dengan memiliki banyak prosesor, perifarel, dan software yang memberikan kemampuan *fail-over* untuk mendukung berbagai komponen ketika terjadi kegagalan sistem. Sistem ini dapat memberikan kemampuan *fail-safe* dengan sistem komputertetap beroperasi

di tingkat yang sama. Akan tetapi, sistem komputer pentoleransi kegagalan menawarkan kemampuan *fail-soft* yang memungkinkan sistem komputer terus beroperasidalam tingkat yang rendah tetapi dapat diterima jika ada kegagalan sistem yang besar.

Tanggung jawab manajemen yang paling penting adalah memastikan keamanan dan kualitas aktivitas bisnisnya yang dijalankan melalui teknologi informasi, maka diperlukan sistem keamanan yang tepat dan dapat mendukung kegiatan dari perusahaan.

2.4. E-Commerce

E-bisnis (Inggris: *Electronic Business, atau "E-business*") dapat diterjemahkan sebagai kegiatan bisnis yang dilakukan secara otomatis dan semiotomatis dengan menggunakan sistem informasi komputer. E-bisnis memungkinkan suatu perusahaan untuk berhubungan dengan sistem pemrosesan data internal dan eksternal mereka secara lebih efisien dan fleksibel. E-bisnis juga banyak dipakai untuk berhubungan dengan suplier dan mitra bisnis perusahaan, serta memenuhi permintaan dan melayani kepuasan pelanggan secara lebih baik. Dalam penggunaan sehari-hari, e-bisnis tidak hanya menyangkut e-dagang (perdagangan elektronik atau *e-commerce*) saja. Dalam hal ini, e-dagang lebih merupakan sub bagian dari e-bisnis, sementara e-bisnis meliputi segala macam fungsi dan kegiatan bisnis menggunakan data elektronik, termasuk pemasaran Internet (e-pemasaran). Sebagai bagian dari e-bisnis, e-dagang lebih berfokus pada kegiatan transaksi bisnis lewat www atau Internet. Dengan menggunakan sistem manajemen pengetahuan, e-dagang mempunyai goal untuk menambah revenue dari perusahaan

Menurut O'brien (2005) *E-commerce* mengubah bentuk persaingan, kecepatan bertindak, dan perampingan interaksi, produk dan pembayaran dari pelanggan ke perusahaan dan dari perusahaan ke pemasok.

Bagi sebagian perusahaan *E-commerce* lebih dari sekedar membeli dan menjual, produk secara online. Sebaliknya, *E-commerce* meliputi seluruh proses dari pengembangan, pemasaran, penjualan, pengiriman, pelayanan, dan pembayaran untuk berbagai produk dan jasa yang diperjualbelikan dalam pasar

global. Teknologi yang digunakan dalam *E-commerce* adalah teknologi informasi dan teknologi internet. Terdapat tiga kategori dasar dalam aplikasi *E-commerce*, yaitu:

1. *E-commerce Business to Consumer (B2C)*

   E-commerce semacam ini, perusahaan harus mengembangkan pasar elektronik yang menarik untuk menjual berbagai produk dan jasa ke para pelanggan.

2. *E-commerce Business to Business (B2B)*

   Katagori ini melibatkan pasar e-business dan hubungan pasar langsung antarperusahaan. Hal lain yang penting juga adalah portal e-commerce B2B yang menyediakan pasar lelang dan jual beli untuk berbagai perusahaan. Perusahaan lain dapat bergantung kepada pertukaran data elektronik (*electronic data interchange*-EDI) melalui internet atau ekstranet untuk pertukaran komputer-ke-komputer atas berbagai dokumen e-commerce dengan para pelanggan besar dan perusahaan pemasoknya.

3. *E-commerce Consumer to Consumer (C2C)*

   C2C *merupakan* sebuah strategi bisnis *e-commerce* yang penting, dengan adanya C2C memudahkan konsumen (dan juga perusahaan) dapat membeli serta menjual ke satu sama lain dalam satu proses.

2.5. CRM *(Customer Relationship Management)*

Sistem kustomisasi *real time* yang memanajemen kustomer dan melakukan personalisasi produk dan servis berdasarkan keinginan konsumen. Menurut O'Brien CRM digunakan untuk mengelola berbagai hubungan pelanggan melibatkan dua tujuan yang saling berkaitan: pertama, memberi organisasi dan semua karyawannya yang berhadapan dengan pelanggan, satu pandangan lengkap tentang setiap pelanggan di setiap hal dan di lintas semua saluran; dan, kedua memberi pelanggan satu pandangan lengkap tentang perusahaan dan saluran-saluran yang lain.

CRM berfokus kepada pelanggan, CRM menggunakan teknologi informasi untuk membuat sistem lintas fungsi perusahaan yang mengitegrasikan dan mengotomatisasikan banyak proses *layanan pada pelanggan* dalam penjualan, pemasaran, dan layanan pelanggan yang berinteraksi dengan pelanggan perusahaan. Sistem CRM menciptakan kerangka kerja TI *software* dan *database*

yang dijalankan melalui Web, yang mengintegrasikan proses-proses dengan operasi bisnis perusahaan lainnya, dan mendukung kerja sama antara perusahaan dengan para pelanggan mitranya.

Potensi manfaat bisnis dari manajemen hubungan pelanggan sangat banyak. CRM memungkinkan sebuah perusahaan untuk mengidentifikasi serta berfokus pada pelanggan terbaik mereka, yaitu mereka yang paling menguntungkan bagi perusahaan agar mereka dapat dipertahankan sebagai pelanggan seumur hidup untuk layanan yang lebih besar dan menguntungkan. Manajemen hubungan pelanggan memungkinkan penyesuaian dan personalisasi *realtime* atas berbagai produk dan jasa berdasarkan pada keinginan, kebutuhan, kebiasaan membeli serta siklus hidup para pelanggan. Manfaat yang besar dari CRM dapat memberikan nilai bisnis strategis bagi perusahaan dan nilai pelanggan yang besar bagi para pelanggannya.

Manfaat bisnis dari manajemen hubungan pelanggan tidak dijamin dan malahan terbukti menjebak bagi perusahaan. Alasan tingginya tingkat kegagalan atau ketidakpuasan dengan usaha yang berkaitan dengan CRM, menunjukan bahwa alasan utamanya adalah kurangnya pemahaman dan persiapan. Dengan kata lain sering kali perusahaan bergantung pada aplikasi baru terkenal dari teknologi informasi (seperti CRM untuk mengatasi masalah bisnisnya tsnps mengembangkan terlebih dahulu perubahan proses bisnis dan program manajemen perubahan yang dibutuhkan).

2.6. *Supply Chain Management* (SCM)

SCM adalah mengintegrasikan praktik manajemen dan teknologi informasi untuk mengoptimalkan informasi dan aliran produk di antara berbagai proses dan mitra bisnis dalam rantai pasokan.

Aplikasi SCM yang dimiliki dipergunakan untuk mengatur dan menyediakan kerja sama untuk seluruh aplikasi/*request* terhadap setiap kebutuhan-kebutuhan dasar pendukung berjalannya sistem, seperti *trading Partners* dan *distribution partners*. SCM di sini meliputi :

- *Demand Management* (perencanaan dan *request* untuk sumber daya segala operasi dalam web (*sales*, *manufacturer*, dan *operation*).

- *Supply Management* (mengatur pemenuhan produk dan layanan untuk setiap pesanan transaksi).
- *Inbound/Outbound Logistic* (pengaturan dan perencanaan sesuatu yang keluar atau masuk ke perusahaan, seperti gudang/*warehouse*).
- *Customer Relationship Management* (CRM). *Customer Interaction* menyediakan layanan bantuan untuk semua pihak dalam komunitas web dalam hal layanan, penawaran, *marketing*, dan transaksi.
- Personalisasi, fokus pada mengenali setiap pengunjung, data customer, dan setiap kegiatannya akan dicatat, sehingga *customer service* bisa melakukan pendekatan yang lebih baik dan menjamin kepuasan *customer*.

Gambar 3. *Supply Chain Management*

III. DATA BASE & SECURITY PADA PERUSAHAAN E-COMMERCE BELIBARANG.COM

3.1. Kebutuhan Data Base Menggunakan *Backward Analysis*

Analisis kebutuhan database pada kasus e-commerce belibarang.com menggunakan metodologi *backward requirement analysis,* yaitu menganalisis kebutuhan *database* dengan penurunan kebutuhan dari fungsi manajemen, tujuan manajemen dan informasi yang dibutuhkan. Fungsi manajemen yang dapat diidentifikasi dari kasus dibagi menjadi 4 fungsi yaitu perencanaan (*planning*), pengarahan (*directing*), aksi *(acting)* dan pengawasan (*monitoring*).

3.1.1. Analisis Kebutuhan Data *(Data Requirement Analysis)*

Analisa kebutuhan data dilakukan berdasarkan business function yang ada dalam belibarang.com yaitu; *E-commerce,* Supply Chain Management dan Customer Relation Management. Kebutuhan *database* diidentifikasikan dengan dengan langkah analisis kebutuhan database berdasarkan urutan sebagai berikut;

- *Management Function,*
- *Management Objectives,*
- *Supporting Information,*
- *Supporting Data,*
- *Sources of Data.*

Belibarang.com yang merupakan obyek bisnis ini membagi 5 kegiatan utamanya yaitu hubungan dengan supplier atau perusahaan pengadaan barang, perencanaan penjualan melalui website, perencanaan distribusi berhubungan dengan perusahaan expedisi, perencanaan transaksi, pembelian peralatan elektronik pendukung.

a. Fungsi Manajemen *(Management Functions)*

Fungsi Manajemen merupakan elemen-elemen dasar yang akan selalu ada dan melekat di dalam proses manajemen yang akan dijadikan acuan oleh pihak dari Belibarang.com dalam melaksanakan kegiatannya untuk mencapai tujuan yang telah di tetapkan. Adapun fungsi manajemen perusahaan terdiri dari

Perencanaan (*Planning*), Pengarahan (*Directing*), Pelaksanaan (*Acting*), Pemantauan (*Monitoring*).

b. Tujuan Manajemen (*Management Objectives*)

Tujuan Manajemen dari Belibarang.com sendiri terdiri dari: Pertama, Perencanaan (P*lanning*) lima kegiatan diatas, yakni :

- Melakukan perencanaan pengadaan produk bekerjasama dengan perusahaan produsen atau supplier, perencanaan produksi website, perencanaan penjualan, perencanaan distribusi, perencanaan transaksi dan pembelian elektronik; pelayanan keluhan pelanggan.
- Pengarahan (*Directing*) dengan kegiatan pengarahan jenis produk dan jumlah kerjasama dengan produsen,, pengarahan kegiatan promosi penjualan, pengarahan kegiatan penjualan, pengarahan jumlah dan jenis produk yang harus didistribusikan, pengarahan jenis transaksi pembelian elektonik yang akan dilakukan; pelayanan keluhan pelanggan
- Pelaksanaan (*Acting*) dengan kegiatan seperti pelaksanaan pengadaan produk yang ditawarkan, pelaksanaan penjualan, pelaksanaan distribusi, pelaksanaan pembayaran elektonik oleh pelanggan; pelayanan keluhan pelanggan.

Pemantauan (*Monitoring*), pemantauan kerjasama dengan pihak lain, pemantauan proses promosi penjualan produk, pemantauan penjualan, pemantauan distribusi produk, pemantauan pembayaran elektronik oleh pelanggan dan juga pemantauan keluhan pelanggan.

c. Informasi Pendukung (*Supporting Information*)

Informasi Pendukung merupakan informasi yang dibutuhkan agar tujuan manajemen dapat tercapai. Informasi pendukung pada fungsi perencanaan (*planning*) yakni Katalog Produk, Daftar Jenis Produk, Rencana Penjualan, Rencana Distribusi, Katalog Bank penyedia jasa elektronik; pada fungsi Pengarahan (*Directing*) terdiri dari Katalog Produsen, Daftar Jenis Produk dan Katalog Produk, Rencana Penjualan, Rencana Alokasi Produk, Katalog Bank penyedia jasa elektonik; pada fungsi Pelaksanaan (*Directing*) terdiri dari Katalog Bahan Baku, Daftar Jenis Produk & Rencana Produksi, Rencana Penjualan,

Rencana Alokasi Produk, Katalog Bank penyedia jasa elektronik; pada fungsi Pemantauan (*Monitoring*) yakni Daftar Pembelian Bahan Baku, Daftar Jenis Produksi & Rencana Produksi, Rencana Penjualan, Rencana Alokasi Produk, Katalog Bank penyedia jasa elektronik serta rencana pelayanan keluhan pelanggan.

d. Data Pendukung (*Supporting Data*)

Data pendukung merupakan data yang dibutuhkan guna diperoleh informasi rencana penjualan yang diinginkan. Data pendukung yang berguna dalam menjalankan fungsi manajemen adalah banyaknya supplier atau produsen, Jumlah dan jenis barang yang dijual, Harga, Harga Produk, Fee, Jenis Pembayaran, Jenis Produk Elektronik Perbankan, Data Kartu kredit, Permintaan Konsumen, Waktu Kirim produk, Nilai dan cara Pembayaran, Jumlah Produk yang dibeli, jumlah keluhan pelanggan yang diterima oleh perusahaan.

e. Sumber Data (*Sources of Data*)

Sumber data dapat diperoleh dari internal dan eksternal perusahaan. Data Internal perusahaan digunakan berasal dari website seperti Jenis, Harga, -Produk, Jenis Pembayaran, Lokasi Penjualan, Permintaan konsumen, sedangkan dari eksternal perusahaan sendiri berasal dari Supplier produk, Produsen, Bank Mitra Kerja seperti Jenis, Harga, Stok Bahan Baku, Jenis, Konsumsi Bahan Baku, Jenis Produk Elektronik Perbankan, Data Kartu Kredit, Nilai Pembayaran, Jumlah Produk Beli.

Secara ringkas analisa kebutuhan data menggunakan backward analysis terlihat dalam tabel berikut :

Tabel 1. Kebutuhan Data Base Menggunakan Backward Analysis

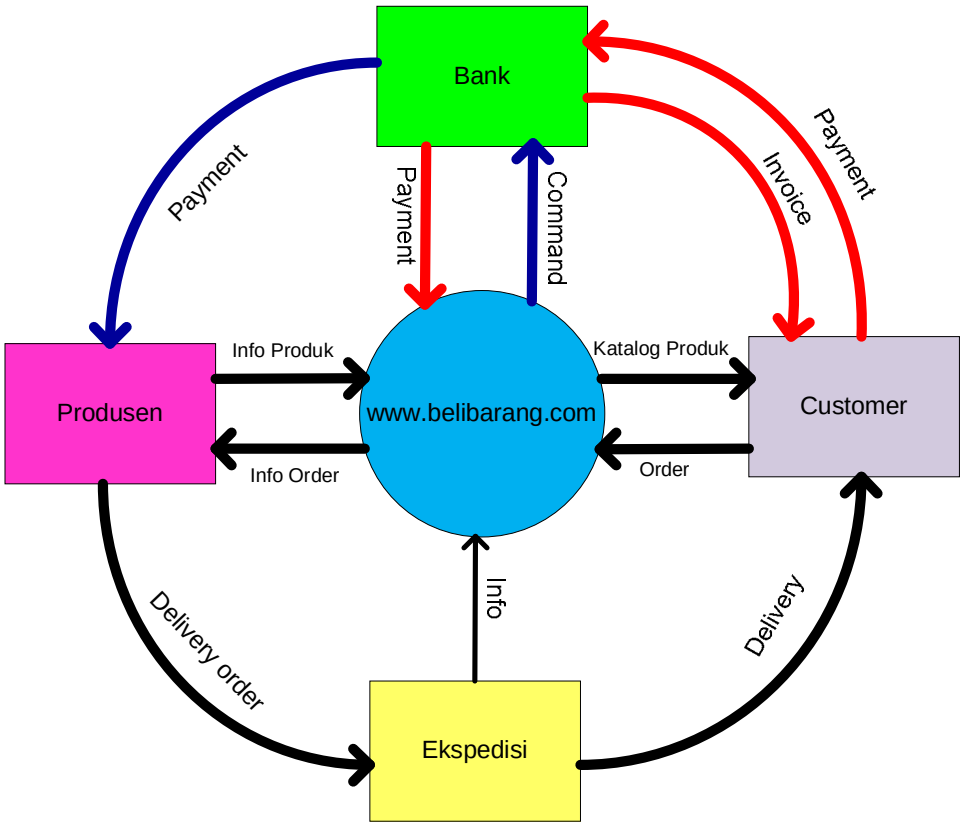
No	Fungsi Manajemen	Tujuan Manajemen	*Suporting Information* (Informasi Pendukung)	*Supporting Data* (Jenis Data)	*Source of Data* (Sumber Data)
1	*Planning*	- Perencanaan pengadaan produk	- Katalog Produk dari Supplier	- Jenis produk - Jumlah stock produk - Harga produk	Supllier produk
		- Perencanaan Penjualan	- Rencana Penjualan	- Jenis produk - Konsumsi produk / jumlah penjualan	Perusahaan belibarang.com
		- Perencanan Promosi	- Rencana Promosi	- Jenis Produk - Harga Produk - Jenis Pembayaran	Perusahaan belibarang.com
		- Perencanaan Distribusi	- Rencana Distribusi	- Jenis produk - Alokasi produk	Perusahaan belibarang.com
		- Perencanaan Transaksi Pembelian elektronik	- Jenis layanan transaksi elektronik Bank mitra kerja	- Jenis produk elektronik perbankan - Data Kartu Debit atau Kredit pembeli	Bank Mitra Kerja
		- Perencanaan Pelayanan Keluhan	- Trend keluhan pelanggan	- Jumlah keluhan pelanggan	Perusahaan belibarang.com
2	*Directing*	- Pengarahan jenis dan jumlah produk yang harus dipromosikan	- Katalog produk	- Jenis produk - Jumlah stock produk - Harga produk	Perusahaan belibarang.com
		- Pengarahan jumlah dan jenis produk yang harus dijual	- Katalog produk - Trend penjualan	- Jumlah stock produk - Jumlah penjualan	Perusahaan belibarang.com
		- Pengarahan kegiatan penjualan	- Rencana Penjualan	- Jenis Produk - Harga Produk - Jenis Pembayaran	Perusahaan belibarang.com
		- Pengarahan jumlah dan jenis produk yang harus didistribusikan	- Rencana Alokasi Produk	- Jenis Produk - Lokasi Penjualan - Permintan konsumen	Perusahaan belibarang.com
		- Perencanaan Jenis Transaksi Pembelian elektronik yang akan dilakukan	- Katalog jenis pembayaran dari bank mitra	- Jenis produk elektronik perbankan - Data Kartu Debit atau Kredit pembeli	Bank Mitra Kerja Pelanggan/konsumen
		Pengarahan Pelayanan Keluhan Pelanggan	- Trend keluhan pelanggan	- Data keluhan pelanggan	Perusahaan belibarang.com

Tabel 1. Kebutuhan Data Base Menggunakan Backward Analysis

No	Fungsi Manajemen	Tujuan Manajemen	*Suporting Information* (Informasi Pendukung)	*Supporting Data* (Jenis Data)	*Source of Data* (Sumber Data)
3	*Acting*	- Pelaksanaan pengadaan barang	- Katalog produk	- Jenis produk - Jumlah Stok produk - Harga produk - Waktu kirim produk	Supllier produk
		- Pelaksanaan penjualan	- Rencana Penjualan	- Jenis Produk - Harga Produk - Jenis Pembayaran - Stok Produk	Perusahaan belibarang.com
		- Pelaksanan distribusi produk	- Rencana Alokasi Produk	- Jenis Produk - Lokasi Penjualan - Permintan konsumen (Jumlah dan Jenis)	Perusahaan belibarang.com
		- Pelaksanan pembayaran elektronik oleh pelanggan	- Katalog Bank penyedia jasa elektronik	- Jenis produk elektronik perbankan - Data Kartu Debit atau Kredit pembeli - Jenis Produk - Harga produk	Bank Mitra Kerja Pelanggan/konsumen
		- Pelaksanan pelayanan keluhan pelanggan	- Keluhan pelanggan	- Daftar keluhan pelanggan	Perusahaan belibarang.com
4	*Monitoring*	- Pemantauan penerimaan bahan baku	- Daftar pembelian produk	- Jenis Bahan Baku - Stok Bahan Baku - Waktu kirim bahan baku	*Supllier* produk
		- Pemantauan proses produksi	- Daftar Jenis Produk - Rencana Produksi	- Stok Produk (barang jadi) - Konsumsi Bahan Baku	Pengusaha belibarang.com
		- Pemantauan penjualan	- Rencana Penjualan	- Jenis, harga dan jumlah stock Produk - Jenis Pembayaran - Jumlah permintaan dan Jenis Pembayaran	Pengusaha belibarang.com Konsumen/pelanggan
		- Pemantauan distribusi produk	- Rencana Alokasi Produk	- Jenis Produk - Lokasi Penjualan - Permintan konsumen (Jumlah dan Jenis)	Pengusaha belibarang.com Pelanggan/konsumen
		- Pemantuan pembayaran elektronik oleh pelanggan	- Katalog Bank penyedia jasa elektronik	- Jenis produk elektronik yang dipilih konsumen - Jumlah produk yang dibeli - Nilai pembayaran	Bank Mitra Kerja Pelanggan/konsumen
		- Pemantauan Keluhan Pelanggan	- Feedback dari pelanggan	- Daftar feedback dari pelanggan	Perusahaan belibarang.com

3.1.2. Keterkaitan Antar Data

Berikut adalah gambar keterkaitan antar data dalam aktivitas Pengusaha Belibarang.com adalah :



Gambar 4. Hubungan Keterkaitan Data

Pada saat penyedia layanan dalam hal ini belibarang.com membutuhkan produk dan harga produk, dengan mengakses field ID_SUPPLIER maka kebutuhan tersebut dipenuhi oleh supplier yang telah menjadi mitra yang secara otomatis teritegrasi melalui sebuah software ERP. Produsen atau supplier juga memiliki filed KONSUMSI_PRODUK untuk mengetahui jumlah produk yang dijual serta posisi terakhir dari produk yang telah dikirimkan kepada pelanggan melalui perusahaan expedisi. Posisi terakhir barang dapat diketahui oleh supplier maupun belibarang.com karena secara otomatis juga terintegrasi dengan software ERP yang ada di perusahaan expedisi. Ketika Pelanggan disuatu daerah ingin membeli produk maka, dengan akses user ID yang telah diberikan oleh penyedia jasa melalui konfirmasi dari pihak bank maka akan didapatkan jenis, harga, dan

jumlah produk yang diinginkan oleh pelanggan tersebut dan produsen juga menyediakan jenis pembayaran bagi pelanggan ketika akan membayar produk tersebut. Cara ini dimungkinkan karena Pengusaha telah bermitra dengan Bank ditunjuk untuk melakukan transaksi keuangan dengan pelanggan. Bank Mitra ini mempunyai ID_ PELANGGAN. Pihak bank akan melakukan pembayaran kepada supplier berdasarkan perintah otomatis dari perusahaan belibarang.com.

3.2. Data Security

Keamanan akan data dan transaksi sangat penting dalam bisnis berbasis teknologi informasi khususnya e-comerce yang seluruh aktivitasnya bergantung pada teknologi. Keamanan ini mencakup semua proses mulai dari pemesanan barang hingga pembayaran. Apabila Belibarang.com tidak dapat meyakinkan konsumen akan keamanan usaha menggunakan system e-commerce ini, maka usahanya akan sulit untuk berkembang, karena tidak ada konsumen yang akan melakukan transaksi dengan usaha ini karena takut akan ketidakamanan tramsaksinya. Maka dari itu perlu perencanaa kemanan yang baik sehingga terpecaya.

3.2.1. Kerawanan Data

Perkembangan sistem informasi yang pesat dewasa ini memungkinkan terwujudnya berbagai kemudahan bagi sebuah organisasi bisnis ataupun perusahaan. Bahkan sistem informasi telah memberikan andil yang sangat besar bagi keberhasilan suatu bisnis. Hal tersebut telah menjadikan sistem informasi ditempatkan sebagai media untuk memenangkan persaingan bisnis di tengah pasar yang semakin kompetitif.

Dibalik kemudahan yang ada, dalam perkembangannya sat ini sistem informasi tidak terlepas dari usaha pihak-pihak yang tidak bertanggung jawab untuk memanfaatkan sistem informasi sebagai sarana memperkaya diri dengan melakukan kejahatan teknologi informasi. Adapun bentuk-bentuk kerawanan data yang dapat terjadi antara lain adalah:

A. Kerawanan Data Pada Skope Elektronik:

1. Kerusakan Data (*data damage*)

   Secara fisik data tidak hilang tetapi data tersebut tidak dapat diakses atau tidak dapat diterjemahkan secara benar. Kerusakan data dapat terjadi secara keseluruhan atau sebagian saja.

2. Data yang tidak dapat diakses

   Maksudnya adalah, secara fisik data ada di dalam media penyimpan data dan tidak mengalami kerusakan, tetapi lokasi data tersebut tidak dapat ditemukan di dalam media penyimpan data tersebut.

3. Data disadap atau dicuri
4. Penyalinan data secara ilegal
5. Pengaksesan data yang terlarang

   Dalam hal ini, pemakai mengakses data yang tidak ada hak akses padanya (tidak berwenang).

6. Terjadinya penyalahgunaan data (*data abuse*)

   Data dapat diakses oleh seseorang tetapi dipergunakan untuk keperluan yang terlarang.

B. Kerawanan data pada Skope Fisik:

1. Tidak stabilnya arus listrik

   Fungsi operasional peralatan komputer sangat tergantung dari pasokan arus listrik, apabila terjadi gangguan arus listrik maka operasional komputer dapat terganggu, bahkan bila arus listrik tersebut secara mendadak terputus sedangkan komputer belum dalam keadaan mati/off, akan dapat merusak perangkat elektronik komputer.

2. Adanya interfensi sinyal, biasanya berasal dari alat elektronik yang bekerja secara tidak normal atau terdapatnya alat pemancar bertegangan tinggi yang menghasilkan interfensi sinyal yang dapat mengganggu kerja komputer.
3. Banjir dan air dapat menyebabkan kerusakan komputer dan data.
4. Petir dapat merusak komponen elektronik komputer pengolah data dan alat komunikasi data.
5. Api dan bahaya kebakaran dapat merusak komputer, data yang tersimpan dalam media dan ruang penyimpan data.

6. Gas, debu, suhu, kelembapan dan zat kimia dapat mengganggu proses kerja dan merusak komputer.
7. Kemungkinan terjadinya pencurian dan aksi ilegal terhadap fasilitas dan peralatan komputer dari sekelompok orang yang tidak bertanggung jawab.
8. Kerusakan peralatan komputer yang diikuti oleh kerusakan data yang tersimpan beserta ruang penyimpan data, yang disebabkan karena umur teknisnya.
9. Kerusakan data akibat penataan kabel dari perangkat komputer yang tidak cermat.

C. Kerawanan Data Pada Skope Prosedural

1. Kehilangan Data (*data losses*)

   Kehilangan data terjadi apabila seluruh atau sebagian data beserta salinannya tidak dapat ditemukan.
2. Data Terhapus
3. Kesalahan pemasukan data
4. Data usang (data tidak *valid*)

   Maksudnya data hanya berlaku benar pada waktu yang lalu tetapi tidak berlaku benar pada saat ini.
5. Data yang tidak dapat diterjemahkan

   Secara fisik data terdapat dalam memori dan tidak rusak tetapi tidak diterjemahkan dengan benar.

3.3. Perencanaan Pengamanan

Dengan perencanaan pengamanan yang baik akan memberikan manfaat usaha yang optimal, sehingga usaha dapat berjalan dan berkembang dengan cepat tanpa hambatan yang krusial seperti kelemahan pada system pengamanan. Konsumen akan merasa aman dan nyaman untuk bertransaksi melalui usaha teknoligi informasi ini.

3.3.1. Pengamanan Data Pada Skope Elektronik:

1. Kerusakan Data (*data damage*)

Dalam mengantisipasi kerusakan data selalu menggunakan antivirus yang reliable dan harus selalu diperbaharui anti virusnya sesuai dengan perkembangan teknologi informasi.

2. Data yang tidak dapat diakses

   Penggunaan *password* dengan sebagaimana mestinya, tidak diperkenankan memberikan kesempatan kepada orang lain untuk mengenali *password* yang dimiliki. Karena pada umumnya kerawanan data berupa data yang tidak dapat diakses ini dikarenakan adanya proteksi *password* serta hak akses. Kemudian informasi perpindahan data harus jelas dan terbuka, karena bisa saja tidak dapatnya suatu data diakses dikarenakan terjadinya perubahan tempat penyimpanan data yang tidak diketahui oleh penggunanya.

3. Data disadap atau dicuri

   Data yang disadap atau dicuri tersebut tidaklah akan berarti bagi pelaku jika data tersebut tidak dapat dibacanya. Oleh sebab itu sebagai langkah pengamanan dapat dipergunakan alat *encryption*. Data yang dikirim melalui encryption hanya dapat dibaca atau diterjemahkan menggunakan alat encryption yang sejenis. Penggunaan encryption dapat beupa alat (fisik) atau dapat berupa suatu program, sandi atau password tertentu yang dikenal dengan istilah *public key* atau *bilateral key exchange*. Penggunaan *public key* atau *bilateral key exchange* yang tidak sesuai dengan daa yang ditetapkan tidak akan dapat membuka atau menerima data.

4. Penyalinan data secara ilegal

   Metode pengamanan sistim ini adalah disamping memperkuat sistem network, sebaiknya benar-benar dilakukan hukum yang menindak tegas pelaku kejahatan komputer seperti ini, sehingga pihak-pihak yang tidak bertanggung jawab tersebut akan berpikir dua kali sebelum melakukan kejahatan komputer, mengingat ganjaran yang harus ditrima karena melanggar hukum yang berlaku.

5. Pengaksesan data yang terlarang

   Metoda pengamanan: membentuk *firewall*, yang berfungsi sebagai penjaga pintu jejaring, dimana hanya komputer yang terdaftar saja yang dapat melalui *firewall* (Turton, 2002). Komputer yang alamatnya tidak terdaftar dalam *firewall* tidak akan dapat masuk dalam sistem jejaring. Fasilitas yang

disediakan *firewall* adalah penggunaan NAT (*Network Address Table*) dimana alamat komputer yang akan berhubungan dengan pihak luar akan disembunyikan agar alamat sesungguhnya tidak diketahui oleh orang lain. Penggunaan *firewall* untuk hubungan dengan pihak luar sangat diperlukan untuk keamanan sistem informasi. Bahkan beberapa koneksi dengan pihak ketiga mewajibkan tersedianya *firewall* untuk dapat mengakses sistem jejaringnya.

6. Terjadinya penyalahgunaan data (*data abuse*)

   Metoda Pengamanan: menerapkan sistem manajemen jejaring. Penggunaan perangkat lunak seperti penggunaan NMS (*Network Management System*) yang berfungsi untuk memonitor jejaring dalam memantau data serta memberikan pengamanan pada sistem informasi (O'Brien, 1999). Penggunaan perangkat lunak ini selain memonitor aktifitas komputer yang terdaftar pada alamat tertentu juga membantu dalam memonitor kondisi kapasitas seluruh komputer yang dipergunakan, sehingga dapat memberikan peringatan dini terhadap kondisi komputer yang digunakan. Pencegahan terhadap penggunaan aplikasi yang tidak standar dapat dilakukan sejak dini dengan bantuan perangkat lunak ini.

3.3.2. Kerawanan data pada Skope Fisik:

1. Tidak stabilnya arus listrik

   Metoda pengamanan: Untuk memberikan pasokan listrik yang handal maka pasokan listrik dapat diperoleh dari PLN dan generator set (genset), biasanya penggunaan genset hanya sebagai *back up* dari pasokan PLN bila terjadi gangguan.

   Sedangkan untuk menjaga agar disaat terjadi perpindahan sumber daya listrik dari PLN ke genset atau sebaliknya tidak terjadi interupsi pasokan daya listrik diperlukan tersedianya UPS (*Up-interrupt Power Supply*). Beberapa merek UPS selain mempunyai kemampuan untuk menyimpan arus listrik juga mempunyai kemampuan untuk menjaga kualitas tegangan listrik yang dihasilkan. Agar kualitas sumber tegagan listrik baik dari PLN maupun genset terjaga tegangannya perlu adanya perangkat *stabilizer*.

2. Adanya interfensi sinyal

   berasal dari alat elektronik yang bekerja secara tidak normal atau terdapatnya alat pemancar bertegangan tinggi yang menghasilkan interfensi sinyal yang dapat mengganggu kerja komputer.

3. Banjir dan air dapat menyebabkan kerusakan komputer dan data

   Metoda pengamanan: Agar komputer, data yang tersimpan dalam media dan ruang penyimpan data terhindar dari bahaya banjir, maka peralatan fisik tersebut ditempatkan pada daerah yang cukup tinggi, sedangkan untuk mengamankan dari bahaya air maka sistem pembuangan instalasi AC dirancang sedapat mungkin tidak mengganggu fasilitas fisik tersebut.

4. Petir dapat merusak komponen elektronik komputer pengolah data dan alat komunikasi data.

   Metoda pengamanan: Gedung dimana tempat komputer pengolah data berada haruslah memiliki peralatan penangkal petir. Ketentuan untuk instalasi penangkal petir memiliki *grounding* dibawah 1 (sesuai dengan standar dari Badan Standarisasi Nasional 2000).

5. Api dan bahaya kebakaran dapat merusak komputer, data yang tersimpan dalam media dan ruang penyimpan data

   Metoda pengamanan: Sistem pengendali api yang dianjurkan untuk ruang komputer tidak menggunakan sistem pemadam air dengan pertimbangan untuk keamanan manusia dan peralatan komputer serta data. Oleh karenanya sistem pengendali api yang dapat digunakan adalah pemadam api berwujud gas (campuran antara nitrogen 87% dan oksigen 12,5%). Sistem pemadam api harus bekerja secara otomatis sehingga dapat memberitahukan adanya kebakaran dengan tanda lampu dan bunyi bel.

6. Gas, debu, suhu, kelembapan dan zat kimia dapat mengganggu proses kerja dan merusak komputer**.**

   Metoda pengamanan: dapat menggunakan sistem pegendali suhu dan kelembapan. Untuk itu diperlukan adanya alat pendingin ruangan (AC) yang spesifikasi suhunya berada antara 16°C-20°C dan kelembapan antara 45% - 55% RH. Fasilitas fisik juga harus terlindung dari cahaya atau sinar matahari langsung serta terlindung dari zat-zat kimiawi.

7. Kemungkinan terjadinya pencurian dan aksi ilegal terhadap fasilitas dan peralatan komputer dari sekelompok orang yang tidak bertanggung jawab.

   Metoda pengamanan: Pengamanan fasilitas fisik dari perbuatan pencurian dan aksi ilegal lainnya dilakukan dengan:

   a. sistem kontrol akses ruangan (*Access Control System*) adalah sistem kontrol untuk akses ke ruang komputer pengolah data dan ruang penyimpan data. Mekanismenya menggunakan kartu identity (*Access Card*) untuk dapat masuk ke ruangan. Identitas pengakses haruslah terlebih dahulu terdaftar pada *access right* yang disimpan pada aplikasi komputer *access control system*, sehingga hanya pihak yang mempunyai akses saja yang dapat masuk ke ruang tersebut.
   b. Sistem monitoring ruangan untuk memantau akifitas ruangan menggunakan *Closed Circuit Television* (CCTV) dengan peralatan ini maka seluruh aktifitas pada ruangan akan termonitor dan terekam dengan sendirinya.

8. Kerusakan peralatan komputer yang diikuti oleh kerusakan data yang tersimpan beserta ruang penyimpan data, yang disebabkan karena umur teknisnya.

   Metoda pengamanan: Pengamanan terhadap kerusakan akibat umur teknis dilakukan dengan melakukan pemeliharaan rutin, misalnya antara 3 sampai 6 bulan sekali dalam setahun agar secara teknis peralatan komputer yang ada masih dapat beroperasi dengan baik. Upaya pemeliharaan itu dapat dilakukan dengan menggunakan jasa *outsourcing* yang memiliki pengalaman dibidangnya. Atau mengganti fasilitas fisik tersebut dengan peralatan yang baru.

9. Kerusakan data akibat penataan kabel dari perangkat komputer yang tidak cermat.

   Metoda pengamanan: Pemasangan dan pengaturan kabel komunikasi data harus segera dilakukan dengan memperhatikan penomoran kabel, efisiensi penggunaan kabel serta terlindungnya kabel dari serangga, tikus atau sebab lain yang membuat kabel dapat terkoyak atau terputus.

3.3.3. Penanganan Data Pada Skope Prosedural

1. Kehilangan Data (*data losses*)

   Metode pengamanan: Buat back *up* data pada beberapa media penyimpan data. Selain itu kontrol terhadap kualitas (performance) kerja processor (CPU) juga diperlukan, dimana menurut standar kualitas kerja processor tidak boleh melebihi 70% (ACI Tandem Computer Inc, 2002) dari kemampuan kapasitasnya CPU.

2. Data Terhapus

   Metoda Pengamanan dengan cara melakukan sosialisasi terhadap prosedur pengolahan data. Sosialisasi ini harus selalu dilakukan baik dimasukkan dalam proses pembelajaran di program pendidikan, training serta program lainnya. Selain itu juga dapat melakukan kontrol terhadap proses *restore* dan *back up* data, agar tidak terjadi kesalahan atau kerusakan data. Dimana proses penyimpanan data tersedia pada mesin back up.

3. Kesalahan pemasukan data

   Metoda Pengamanan: Kontrol aplikasi proses, seperti adanya sistem isyarat dini untuk memastikan bahwa proses yang akan dilakukan adalah benar. Sebagai contoh sistem sistem isyatrat dini adalah jika akan dilakukannya proses tutup hari (end off day) sistem akan memberikan informasi bahwa yang akan dilakukan adalah proses tutup hari, bukan proses tutup tengah hari (*mid of day*) atau bukan juga proses awal hari (*start on day*). Contoh lain adalah tersedianya *message error* bila terjadi kesalahan pada jalannya proses atau terhadap kegagalan proses seperti tidak terprosesnya suatu data tertentu.

4. Data usang (data tidak *valid*)

   Metoda pengamanan: melakukan sistem pemutakhiran data (*data up to date*) dan pengolahan data (*data processing*) dengan baik dan benar. Oleh karenanya perlu dibentuk unit tersendiri yang menangani masalah terkait dengan pembuatan prosedur dan administrasi dokumen karena tanpa unit tersendiri ini maka pembuatan prosedur dan administrasi dokumen tidak akan pernah selalu *up-to date*.

5. Data yang tidak dapat diterjemahkan

Metoda pengamanan: Menerapkan penggunaan *encryption* yang benar dan sesuai prosedur, dan jika memang diperlukan dapat memanfaatkan aplikasi berbasis web base seperti portal atau dokumen manajemen yang dapat dipergunakan sebagai sarana menampung prosedur-prosedur yang dapat diakes oleh seluruh karya

IV. KESIMPULAN

Berdasarkan rencana pembuatan data base manajemen untuk belibarang.com, dapat disimpulkan beberapa hal sebagai berikut :

1. Dalam analisis database yang menggunakan metodologi backward requirement analysis, diperlukan analisis kebutuhan dari fungsi manajemen, tujuan manajemen dan informasi yang dibutuhkan. Kebutuhan database diidentifikasikan dengan urutan langkah analisis kebutuhan database berdasarkan Management Function, Management Objectives, Supporting Information, Supporting Data, Sources dari perusahaan yang merupakan obyek bisnis ini membagi 5 kegiatan utamanya yaitu pengadaan produk, perencanaan produk, perencanaan penjualan, perencanaan distribusi, perencanaan transaksi, pembelian elektronik.
2. Dengan menggunakan Fungsi manajemen dari Perencanaan (Planning), Pengarahan (Directing), Pelaksanaan (Acting), Pemantauan (Monitoring). Maka perusahaan belibarang.com akan mampu melakukan efisiensi dan efektivitas dalam pelayanannya. Sedangkan dalam analisis keterkaitan data Perusahaan akan mampu terkoneksi antara suplier, pelanggan dan bank mitra dan dapat terkoneksi secara real time. serta dapat memberikan fleksibilitas akses ke pelanggan dalam pembelian atau penyediaan produk *e-commerce.*
3. Kerawanan data bisa terjadi dalam proses bisnis yang diakibatkan terjadinya kejahatan komputer. Kerawanan data bisa terjadi secara elektronik, secara fisik, maupun secara prosedural sehingga diperlukan tata cara pengelolaan data yang sesuai, supaya tidak terjadi kerawanan data. Karena kejahatan komputer merupakan salah satu kejahatan yang sulit dideteksi dan dilacak keberadaannya. Kerawanan data ini bisa terjadi apabila sistem yang digunakan tidak memperhatikan pengamanan data. Untuk menghidari kerawanan data baik itu secara elektronik, fisik maupun prosedural diperlukan perencanaan pengamanan data, baik itu secara elektronik, fisik ataupun prosedural, diperlukan pengamanan data sehingga kemungkinan untuk terjadinya kehilangan data akan diminimalisir.

DAFTAR PUSTAKA

Marimin. 2006. Sistem Informasi Manajemen pada Sumber Daya Manusia. Grasindo. Jakarta

Modul Mata Kuliah Sistem Informasi Manajemen. 2011. Program Studi Manajemen dan Bisnis, Sekolah Pascasarjana, Institut Pertanian Bogor.

O Brien, dkk. Manajemen Sistem Informasi. Prentice Hall. 2006

Oetomo, Budi Sutedjo Dharma. 2002. Perencanaan dan Pembangunan Sistem Informasi. Penerbit Andi. Yogyakarta.

http://www.techrepublic.com/blog/10things/10-tips-for-securing-a-microsoft-access-database/552

http://oracle-magician.blogspot.com/2008/05/how-to-secure-oracle-10g11g-enterprise.html

http://coolthingoftheday.blogspot.com/2011/06/secure-database-applications-with.html

http://integrant.com/2011/05/26/tips-for-securing-your-database-server-mssql-2008-transparent-data-encryption/

http://christopherickes.com/web-app-development/secure-php-database-access/

http://www.depesz.com/index.php/2007/08/18/securing-your-postgresql-database/

http://www.blogging-secret.com/how-to-solve-error-establishing-a-database-connection-for-wordpress

http://searchsecurity.techtarget.com/tip/Five-tips-for-secure-database-development

http://it.toolbox.com/blogs/david/the-secure-oracle-database-25158

http://blogs.kuppingercole.com/kuppinger/2011/03/16/database-security-a-hot-topic/

http://srmsblog.burtongroup.com/database_security/

http://www.miroconsulting.com/blog/index.php/category/database-security/

http://technology.amis.nl/blog/7796/an-evening-with-oracle-database-security-expert-pete-finnigan

http://yanitaita.blogspot.com/2010/07/aplikasi-security-code-sederhana-untuk.html

http://heyratna.wordpress.com/2010/10/10/perkembangan-basis-data/

http://kumpulantutorial.blogspot.com/2007/12/isu-isu-keamanan-basisdata.html

http://blog.binadarma.ac.id/mutakin/?p=152

http://amokdarmianto.wordpress.com/2010/10/25/keamanan-database

http://www.ari.haryadi.web.ugm.ac.id/?p=9

http://yurindra.wordpress.com/about/keamanan-basisdata/#comment-721

http://createino.blogspot.com/2008/06/keamanan-basis-data.html?

http://lucamerolla.wordpress.com/2011/06/16/stand-alone-hornetq-security-database-module/

http://blog.uin-malang.ac.id/ivageje/2011/05/13/keamanan-database/comment-page-1/#comment-983

http://www.blogger.com/comment.g?blogID=8419749188710286139&postID=586117714901019986 6&page=1&token=1311550555213