Karya Ilmiah

PEMELIHARAAN KEAMANAN FISIK ATAS KONTROL FASILITAS SISTEM KOMPUTER

Oleh :

Hendryan Winata, S.Kom., M.Kom.

SEKOLAH TINGGI MANAJEMEN ILMU KOMPUTER
TRIGUNADARMA
MEDAN
2012

BAB I

PENDAHULUAN

1.1. Latar Belakang

Ranah persoalan (domain) keamanan fisik (physical security) dalam keamanan sistem informasi amatlah jelas dan ringkas. Domain kemanan fisik menguji elemen-elemen lingkungan fisik dan infrastruktur pendukung yang menjaga kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) sebuah sistem informasi. Di sini tidak dibahas mengenai logical control, akan tetapi beberapa physical control yang dideskripsikan di sini dalam beberapa domain lainnya, seperti operation control, dan access control. Bencana alam adalah contoh ancaman fisik pada keamanan. Kontrol fasilitas terhadap akses yang tidak berwenang atau pencurian adalah elemen dari keamanan fisik. Area yang dikenal sebagai indsutrial security banyak mengenal hal-hal demikian, seperti CCTV (Closed-Circuit Television), penjagaan, pemagaran, pencahayaan, dan sebagainya.

Domain keamanan fisik membahas ancaman, kerawanan, dan tindakan yang dapat diambil untuk memberi perlindungan fisik terhadap sumber daya organisasi dan informasi yang sensitif. Sumberdaya ini meliputi personel, fasilitas tempat mereka bekerja, data, peralatan, sistem pendukung,

dan media yang mereka gunakan,. Keamanan fisik sering mengacu pada tindakan yang diambil untuk melindungi sistem, gedung, dan infrastruktur pendukung yang terkait terhadap ancaman yang berhubungan dengan lingkungan fisik. Keamanan fisik komputer dapat juga didefinisikan sebagai proses yang digunakan untuk mengontrol personel, bangunan fisik, peralatan, dan data yang terlibat dalam pengolahan informasi.

1.2. Tujuan Penulisan

Penulisan karya ilmiah ini bertujuan untuk mengetahui pemeliharaan keamanan fisik atas kontrol fasilitas sistem komputer.

BAB II

URAIAN TEORITIS

2.1. Ancaman pada Physical Security

Sebelum memulai berbagai macam investigasi dan antisipasi terhadap keamanan, kita perlu mengetahui aspek apa saja dari lingkungan yang bisa mengancam infrastruktur komputer. Ketika analisa resiko atau penilaian dampak bisnis dilakukan, ancaman yang mungkin terjadi harus didaftarkan. Tidak peduli kemungkinan terjadinya kerawanan tersebut rendah atau tidak mungkin, daftar semua ancaman yang mungkin harus disusun.

Beberapa metode *assessment* seperti CMM atau IAM membuat praktisi melakukan penyusunan daftar yang lengkap atas kemungkinan terjadinya ancaman keamanan fisik. Ketiga aspek CIA juga merupakan resiko yang harus dilindungi oleh keamanan fisik. Beberapa contoh resiko CIA dalam keamanan fisik adalah seperti berikut ini:

1. Interupsi dalam menyediakan layanan komputer—ketersediaan
2. Kerusakan fisik—ketersediaan
3. Keterungkapan informasi—kerahasiaan
4. Kehilangan kendali atas sistem—keutuhan
5. Pencurian—kerahasiaan, keutuhan, dan ketersediaan

Sedangkan beberapa contoh ancaman terhadap keamanan fisik di antaranya:

Emergensi

- Kebakaran dan kontaminasi asap
- Kerusakan bangunan
- Kehilangan fasilitas utilitas /infrastruktur (listrik, AC, dan pemanas)
- Kerusakan jaringan air (perusakan Pipa)
- Limbah atau bahan beracun

Bencana Alam

- Aktivitas pergerakan bumi (gempa, longsor)
- Kerusakan oleh badai (salju, es, dan banjir)

Intervensi Manusia

- Sabotase
- Vandalisme
- Perang
- Serangan

Donn B.Parker dalam Fighting Commputer Crime (Wiley,1998) telah menyusun daftar yang sangat komprehensif yang ia sebut tujuh sumber utama yang menyebabkan kerugian fisik dengan contohnya masing-masing:

1. Temperatur

Suhu panas dan dingin yang bervariasi secara ekstrim seperti sinar matahari, api, pembekuan, dan pemanasan

2. Gas

Termasuk di dalamnya adalah gas yang digunakan dalam perang, gas komersial, kelembapan, udara kering, dan partikel mengambang. Sebagai contoh adalah gas Sarin (gas saraf), asap, kabut, cairan pembersih, uap bahan bakar, dan partikel kertas dari printer.

3. Cairan

Meliputi air dan bahan kimia. Contohnya adalah banjir, kebocoran pipa air ledeng, endapan salju, kebocoran bahan bakar, minuman yang tumpah, bahan kimia pembersih asam dan basa, dan cairan printer.

4. Organisme

Virus, bakteri, manusia, binatang, dan serangga. Misalnya adalah sakitnya pegawai penting, jamur, kontaminasi minyak dari kulit dan rambut, kontaminasi cairan tubuh organisme, dan korslet microcircuit akibat jaring laba-laba

5. Proyektil

Obyek nyata yang bergerak cepat dengan tenaga seperti meteor, benda jatuh, mobil dan truk, peluru dan roket, ledakan, dan angin.

6. Pergerakan bumi

Keruntuhan, kemiringan, goncangan akibat gempa bumi dan lainnya, getaran, aliran lava, gelombang laut, dan tanah longsor yang dapat mengakibatkan jatuhnya atau berguncangnya perangkat yang rentan goncangan sehingga menjadi rusak.

7. Anomali energi

Berbagai tipe anomali listrik adalah gelombang listrik, magnetisme, listrik statik, radiasi, gelombang suara, cahaya, radio, microwave, atom, dan elektromagmetik. Contohnya adalah kegagalan elektrik, kedekatan dengan sumber magnet dan elektromagnet, listrik statik dari karpet, penghancuran kertas dan disk magnetik, *Electro-Magnetik Pulse* (EMP) dari ledakan nuklir, laser, loudspeaker, senjata *High-Energy Radio Frequency* (HERF), sistem radar, radiasi kosmik, dan ledakan.

2.2. Kontrol atas *Physical Security*

Ada beberapa area dalam kontrol keamanan fisik. Secara umum, kontrol ini harus sesuai dengan ancaman yang terdaftar. Dalam bab ini, kontrol keamanan fisik dibagi dalam 3 grup: kontrol administratif, kontrol lingkungan dan keamanan hidup, serta kontrol fisik dan teknis.

2.2.1. Kontrol Administratif

Kontrol administratif, sebagai lawan dari kontrol fisik dan teknis, adalah area perlindungan keamanan fisik yang dilakukan dengan langkah-

langkah administratif. Langkah ini mencakup prosedur emergensi, kontrol personel (dalam area sumber daya manusia), perencanaan, dan penerapan kebijakan. Di bawah ini adalah pembahasan elemen kontrol administratif yang terdiri dari perencanaan kebutuhan fasilitas, manajemen keamanan fasilitas, dan kontrol personel administratif.

a. Perencanaan Kebutuhan Fasilitas

Perencanaan kebutuhan fasilitas adalah konsep akan perlunya perencanaan kontrol keamanan fisik pada tahap awal dari pembangunan fasilitas data. Beberapa elemen keamanan fisik dalam tahap pembangunan meliputi memilih dan merencanakan lokasi site yang aman.

Memilih Site yang Aman

Lokasi lingkungan dari fasilitas juga menjadi pertimbangan dalam perencanaa awal. Beberapa pertanyaan yang perlu dipertimbangkan di antaranya :

- Visibilitas

Lingkungan bertetangga seperti apa sebuah lokasi diajukan? Akankah lokasi tersebut memiliki penanda eksternal yang akan mencirikannya sebagai area yang sensitif? Visibilitas yang rendah adalah keharusan.

- Pertimbangan Lokasi

Apakah tempat yang diajukan berlokasi dekat dengan sumber bahaya (sebagai contoh, tempat pembuangan sampah)? Apakah daerah tersebut memiliki tingkat kriminalitas tinggi?

- Bencana Alam

Apakah tempat tersebut memiliki kemungkinan terjadinya bencana alam yang lebih tinggi dibanding daerah lainnya? Bencana alam bisa termasuk kendala cuaca (angin, salju, banjir, dsb) dan keberadaan lempengan gempa bumi.

- Transportasi

Apakah lokasi tersebut memiliki masalah akibat lalu lintas darat, laut, atau udara yang berlebihan?

- Persewaan bersama

Apakah akses terhadap kontrol lingkungan atau HVAC (*heating, ventilation and air conditioning*) dipersulit dengan adanya tanggungjawab bersama? Sebuah data center tidak boleh memiliki akses penuh ke sistem ketika keadaan emergensi terjadi.

- Layanan Eksternal

Berapakah jarak lokasi dengan layanan emergensi, seperti polisi, pemadam kebakaran, rumah sakit, atau fasilitas medis?

Merancang Site yang Aman

Area sebuah sistem informasi adalah fokus utama dalam kontrol fisik. Contoh area yang perlu mendapat perhatian selama tahap perencanaan pembangunan adalah :

- Tembok

Keseluruhan tembok, dari lantai hingga langit-langit, harus memiliki standar keamanan terhadap kebakaran yang cukup. Lemari atau ruangan yang dijadikan tempat penyimpanan media harus memiliki standar yang tinggi.

- Langit-langit

Masalah yang dipertimbangkan adalah standar kemampuan menahan beban dan standar keamanan terhadap kebakaran

- Lantai

Berikut ini adalah hal yang perlu diperhatikan mengenai lantai:

Lempengan, Jika lantai adalah lempengan beton, pertimbangannya adalah beban yang sanggup didukung (disebut sebagai loading, yang biasanya adalah 150 pon per kaki persegi), dan ketahanannya terhadap api.

Raised, ketahanannya terhadap api, dan materinya yang tidak menghantarkan listrik menjadi pertimbangan.

- Jendela

Jendela biasanya tidak dibuat pada sebuah data center. Jika ada, jendela harus tembus cahaya dan anti pecah.

- Pintu

Pintu pada sebuah data center harus tahan terhadap pembobolan, dan memiliki ketahanan terhadap api yang sama seperti pada tembok. Jalan keluar darurat harus dicirikan dengan jelas, terawasi/termonitor, dan

beralarm. Ketika emergensi, kunci pintu elektrik harus dalam keadaan tidak dapat digunakan jika daya listrik lumpuh agar memungkinkan evakuasi yang aman. Meskipun hal ini dianggap sebagai masalah bagi keamanan, keselamatan personel harus didahulukan, dan pintu ini harus dijaga dalam keadaan darurat.

- Pemancar Air

Lokasi dan tipe sistem pemadaman api harus direncanakan.

- Jaringan pipa dan gas

Katup pipa air dan gas di seluruh bangunan harus diketahui. Begitu pula drainase yang baik, yaitu yang mengalir ke luar bangunan, sehingga tidak membawa zat kontaminan ke dalam bangunan

- AC

Sumber daya listrik untuk AC harus disediakan khusus, dan diketahui dimana lokasi saklar EPO (Emergency Power Off)-nya. Sebagaimana halnya drainase air, udara dari sistem pendingin harus mengalir keluar dengan tekanan udara yang positif, serta memiliki ventilasi yang melindungi fasilitas dari udara yang mengandung racun.

- Kebutuhan Kelistrikan

Fasilitas harus memiliki sumber daya listrik cadangan dan alternatif yang layak. Kontrol akses terhadap panel distribusi listrik harus dijaga.

b. Manajemen Keamanan Fasilitas

Manajemen keamanan fasilitas terdiri dari jejak audit dan prosedur emergensi. Keduanya adalah elemen kontrol keamanan administratif yang tidak berhubungan dengan perencanaan awal penentuan site yang aman, namun dibutuhkan sebagai dasar operasionalnya.

Jejak Audit

Jejak audit atau log audit adalah rekaman kejadian. Sebuah sistem komputer dapat memiliki beberapa jejak audit, yang masing-masing fokus pada jenis kegiatan tertentu seperti mendeteksi pelanggaran keamanan, masalah kinerja serta mendeteksi cacat desain dan pemrograman dalam aplikasi. Dalam domain keamanan fisik, jejak audit dan log kontrol akses adalah penting karena manajemen perlu mengetahui dari mana usaha akses ke sistem dilakukan dan siapa pelakunya. Jejak audit atau log akses harus merekam hal berikut:

- Tanggal dan tempat usaha akses
- Apakah usaha akses berhasil
- Dimana akses diberikan (contoh: pintu yang mana)
- Siapa yang mengusahakan akses
- Siapa yang mengubah hak akses pada level supervisor

Beberapa sistem jejak audit dapat mengirimkan alarm atau tanda pada personel jika usaha ada akses yang berkali-kali gagal dilakukan. Jejak audit

dan log akses adalah pendeteksian dan bukan pencegahan. Keduanya tidak dapat menghentikan penyusupan—meskipun diketahui bahwa jejak audit dari usaha akses yang disusun mungkin mempengaruhi penyusup untuk tidak melakukan usaha akses. Bagaimanapun, jejak audit menolong seorang administrator merekonstruksi detail penyusupan setelah kejadian.

Prosedur Emergensi

Implementasi prosedur emergensi dan pelatihan pegawai serta pengetahuan akan prosedur adalah bagian penting dari kontrol fisik administratif. Prosedur-prosedur ini harus didokumentasikan dengan jelas, siap akses (termasuk salinan yang disimpan di tempat lain pada kejadian bencana), dan di-update secara periodik.

Elemen administrasi prosedur emergensi harus mencakup hal berikut:

- Prosedur shutdown sistem darurat
- Prosedur Evakuasi
- Pelatihan pegawai, pendalaman pengetahuan secara periodik
- Testing sistem dan peralatan secara periodik

Kontrol Personel Administratif

Kontrol personel administratif mencakup proses administratif yang biasa diimplementasikan oleh departemen SDM selama perekrutan dan pemecatan pegawai. Contoh kontrol personel yang diterapkan adalah sebagai berikut:

- Screening pra kepegawaian

Pengecekan sejarah kepegawaian, pendidikan, dan referensi. Penyelidikan latar belakang atau penghargaan untuk posisi yang penting dan sensitif

- Pengawasan kepegawaian

Kejelasan tingkat keamanan—dibuat jika pegawai memiliki akses ke dokumen rahasia. Penilaian atau review pegawai oleh penyelia mereka

- Prosedur pasca kepegawaian

Wawancara ketika pegawai keluar. Penghapusan akses ke jaringan dan penggantian password. Pengembalian inventaris komputer dan laptop.

2.2.2. Kontrol Lingkungan dan Keselamatan Hidup

Kontrol lingkungan dan keselamatan hidup dianggap sebagai kontol kemanan fisik yang dibutuhkan untuk menjamin baik lingkungan operasi komputer maupun lingkungan operasi personel. Hal di bawah ini adalah tiga area utama dari kontrol lingkungan:

a. Daya Listrik

Sistem kelistrikan adalah darah bagi pengoperasian komputer. Suplai listrik kontinyu yang bersih dan stabil dibutuhkan untuk memelihara lingkungan personel yang layak dan juga pengoperasian data. Banyak hal

yang mengancam sistem daya listrik, yang paling umum adalah *noise, brownout,* dan kelembapan.

***Noise**, Noise* dalam sistem kelistrikan mengacu pada adanya radiasi listrik dalam sistem yang tidak dikehendaki dan berinterferensi dengan listrik yang bersih. Beberapa masalah daya listrik telah dibahas dalam Bab 3,"Keamanan Jaringan dan Telekomunikasi", seperti UPS (*Uninterruptable Power Supplies*), dan daya listrik cadangan. Dalam bab ini akan dibahas lebih detil mengenai tipe masalah kelistrikan dan solusi yang direkomendasikan Ada beberapa jenis *noise,* yang paling umum adalah *Electromagnetic Interference* (EMI) dan *Radio Frequency Interference* (RFI). EMI adalah noise yang disebabkan oleh adanya radiasi akibat perbedaan tegangan listrik antara tiga kabel listrik—*hot wire*, kabel netral, dan kabel ground. Dua tipe EMI yang umum disebabkan oleh sistem kelistrikan:

- *common-mode noise*. Noise dari radiasi yang dihasilkan oleh perbedaan tegangan antara *hot wire* dan kabel *ground*
- *traverse-mode noise*. Noise dari radiasi yang dihasilkan oleh perbedaan tegangan antara *hot wire* dan kabel netral.RFI dihasilkan oleh komponen-komponen dalam sebuah sistem kelistrikan, seperti radiasi kabel listrik, pencahayaan dengan fluoresens, dan pemanas listrik. RFI bisa menjadi masalah serius karena tidak hanya tidak hanya menginterferensi

komputer, tapi juga bisa mengakibatkan kerusakan permanen pada komponen yang sensitif.

Beberapa tindakan perlindungan terhadap noise di antaranya adalah:

- Pengkondisian jaringan sistem kelistrikan
- *Grounding* yang baik
- Membatasi kedekatan dengan magnet, cahaya fluorensens, motor listrik, dan pemanas.

Tabel 1. Istilah Gangguan Daya Listrik

Elemen	Deskripsi
Fault	Hilang daya listrik sementara
Blackout	Mati listrik
Sag	Turun tegangan listrik sementara
Brownout	Turun tegangan listrik yang lama
Spike	Naik tegangana listrik sementara
Surge	Naik tegangan listrik yang lama
Inrush	Arus listrik pada waktu permulaan
Noise	Gangguan interferensi yang kontinyu
Transient	Gangguan interferensi sementara
Clean	Arus listrik asal yang tidak naik-turun
Ground	Kabel dalam sirkuit listrik yang disambungkan ke tanah

Brownout

Brownout adalah turunnya tegangan listrik yang agak lama yang bisa menyebabkan kerusakan fisik serius komponen elektronik yang sensitif. ANSI (*American National Standard Institute*) mengizinkan 8 persen penurunan

antara sumber listrik dengan meteran listrik bangunan, dan 3,5 persen penurunan antara meteran listrik dengan colokan listrik.

Sebagai tambahan, *surge* dan *spike* terjadi ketika daya listrik kembali pulih dari penurunan dan kenaikan tegangan yang juga bisa merusak komponen elektronik. Semua komputer harus dilindungi oleh peredam *surge*, dan peralatan penting memerlukan UPS (*Uninterruptable Power Supply*)

Kelembapan

Kelembapan yang aman adalah 40% dan 60%. Kelembapan tinggi yang lebih besar dari 60% dapat mengakibatkan masalah karena membuat pengembunan pada komponen perangkat komputer. Kelembapan tinggi juga membuat masalah dengan pengkaratan pada koneksi elektrik. Proses seperti pengkerakan elektrik terjadi, menyebabkan partikel perak berpindah dari konektor ke sirkuit tembaga sehingga menghambat efisiensi listrik dari komponen.

Kelempapan rendah yang kurang dari 40% meningkatkan potensi kerusakan yang diakibatkan listrik statik. Listrik statik sebesar 4000 volt mungkin terjadi pada keadaan kelembapan normal di lantai yang terbuat dari kayu atau vinyl, dan tegangan listrik statik sebesar 20.000 volt atau lebih

mungkin terjadi jika kelembapan udara sangat rendah pada karpet yang tidak anti listrik statik.

Meskipun cuaca tidak dapat diatur, tingkat kelembapan relatif di ruangan komputer dapat dikendalikan melalui sistem HVAC (*Heating, Ventilation, and Air Conditioning*). Tabel di bawah ini mendaftarkan kerusakan pada perangkat keras komputer akibat listrik statik.

Tabel 2. Kerusakan Akibat Listrik Statik

Tegangan Listrik Statik	Kerusakan
40	Transistor dan sirkuit yang sensitif
1.000	Mengacak tampilan monitor
1.500	Kehilangan data pada disk drive
2.000	Sistem mati
4.000	Printer macet
17.000	Kerusakan permanen pada *chip*

Beberapa tindakan pencegahan yang diambil untuk mengurangi kerusakan akibat listrik statik:

- Menyemprotkan spray anti listrik statik
- Ruangan pusat operasi atau pusat komputer menggunakan lantai anti listrik statik
- Gedung, dan ruangan komputer harus di-*ground* dengan baik
- Menggunakan meja atau karpet anti listrik statik
- Sistem HVAC menjaga tingkat kelembapan yang baik di ruangan komputer

b. Pendeteksian dan Pemadaman Kebakaran

Pendeteksian dan pemadaman kebakaran yang baik mutlak diperlukan untuk keselamatan dan keberlangsungan sistem informasi. Kelas kebakaran, bahan-bahan yang mudah terbakar, detektor, dan metode pemadaman api harus diketahui.

Jenis Api dan Bahan Mudah Terbakar

Pada tabel di bawah ini didaftarkan tiga kelas utama kebarakan, jenis bahan mudah terbakar pada kelasnya masing-masing, dan bahan pemadam yang disarankan.

Tabel 3. Kelas Kebakaran, dan Media Peredam

Kelas	Deskripsi Bahan Penyebab	Medium Peredam
A B	Bahan umum yang mudah terbakar Cairan	Air atau asam soda CO_2, asam soda, atau Halon
C	Listrik	CO_2, atau Halon

Untuk terjadinya oksidasi yang cepat (pembakaran), harus ada tiga elemen: oksigen, panas, dan bahan bakar. Masing-masing medium pemadam mempengaruhi elemen yang berbeda sehingga cocok untuk memadamkan tipe kebakaran yang berbeda pula - Air, Menurunkan suhu yang dibutuhkan api agar tetap menyala.

- Asam soda, Meredam pasokan bahan bakar untuk api.
- CO2, Menurukan kadar pasokan oksigen yang dibutuhkan untuk mempertahankan nyala api.
- Halon, Meredam pembakaran melalui reaksi kimia yang mematikan api.

Detektor Api

Detektor api mengindra panas, nyala api atau asap untuk mendeteksi adanya pembakaran atau hasil samping pembakaran. Tipe detektor yang berbeda memiliki atribut yang berbeda dan digunakan untuk mendeteksi atribut api yang berbeda pula untuk memicu alarm.

- **Pengindra panas**. Perangkat sensor pengindra panas mendeteksi dengan salah satu dari dua keadaan: 1) suhu mencapai ambang batas yang telah ditentukan, atau 2) suhu meningkat cepat tanpa memperhatikan suhu awal. Tipe pertama, perangkat pendeteksi suhu yang tetap, memiliki tingkat kesalahan alarm yang lebih rendah dibanding yang kedua, detektor pendeteksi perubahan suhu.
- **Pemicu api**. Perangkat sensor pemicu api teramat mahal karena mereka mendeteksi baik energi infra merah dari nyala api maupun denyut nyala api namun memiliki waktu tanggap yang sangat cepat. Perangkat ini biasanya digunakan pada aplikasi khusus untuk perlindungan peralatan berharga.
- **Pemicu asap**. Perangkat sensor pemicu asap biasa digunakan pada sistem ventilasi dimana perangkat tersebut sangat berguna. Perangkat fotoelektrik dipicu oleh variasi dalam cahaya yang menerpa sel fotoelektrik sebagai hasil dari keadaan asap. Tipe detektor asap yang lain,

Radioactive Smoke Detection, membangkitkan alarm ketika arus ionisasi yang dihasilkan oleh bahan radioaktifnya diganggu oleh asap.

- **Alarm *Automatic Dial-up Fire.*** Ini adalah tipe mekanisme respon sinyal yang menghubungi nomor telepon pemadam kebakaran atau polisi setempat dan menjalankan rekaman pesan ketika kebakaran terjadi. Alarm ini sering digunakan sebagai tambahan detektor kebakaran yang telah disebutkan sebelumnya. Perangkat ini tidak mahal namun dapat disalahgunakan dengan mudah.

Sistem Pemadaman Kebakaran

Sistem pemadam kebakaran ada dua jenis: sitem penyemprot air dan sistem pelepas gas. Sistem penyemprot air terdiri dari empat variasi

- **Pipa basah**. Sistem penyemprot air pipa basah adalah pipa yang selalu mengandung air, tau disebut juga sistem *close head*. Pada penerapan yang umum jika terjadi kenaikan suhu mencapai 165° F, kait yang dapat luruh pada mulut pipa meleleh menyebabkan katup membuka, memungkinkan air mengalir. Ini dianggap sebagai sistem penyemprot yang paling bisa diandalkan. Bagaimanapun, kelemahan utamanya adalah jika terjadi kegagalan di mulut pipa atau pipa akan menyebabkan kebanjiran, dan pipanya bisa membeku jika terkena cuaca dingin.

- **Pipa kering**. Dalam sistem pipa kering, tidak ada air dalam pipa karena airnya ditahan pada katup klep. Pada keadaan kebakaran seperti yang telah disebutkan di atas, katupnya membuka, udara disemprotkan keluar pipa, dan kemudia air mengalir. Meskipun sistem ini dianggap kurang efisien, namun lebih disukai dibanding pipa basah untuk instalasi komputer karena adanya jeda waktu yang memungkinkan komputer dimatikan terlebih dahulu sebelum sistem pipa kering diaktifkan.
- ***Deluge***. *Deluge* adalah tipe pipa kering, namun volume air yang disemprotkan jauh lebih banyak. Tidak seperti ujung penyemprot *sprinkler*, *deluge* dirancang untuk mengirimkan air dalam jumlah besar pada suatu area dengan cepat. Tidak disarankan untuk peralatan komputer karena membutuhkan waktu lama bagi sistem komputer untuk kembali berjalan setelah kejadian.
- ***Preaction***. *Preaction* adalah sistem penyemprot air yang disarankan untuk ruangan komputer. *Preaction* mengkombinasikan sistem pipa kering dan sistem pipa basah, dengan pertama-tama melepaskan air ke dalam pipa ketika terdeteksi panas (pipa kering), dan kemudian melepaskan aliran air ketika kait pada mulut pipa meleleh (pipa basah).

Medium Peredam

- Karbon Dioksida (CO2). CO2 adalah gas yang tidak berwarna dan tidak berasa yang digunakan dalam pelepasan gas pada sistem pemadam

kebakaran. CO2 sangat efektif dalam memadamkan api karena faktanya gas ini dengan cepat menghilangkan oksigen yang digunakan dalam prose pembakaran ketika terjadi kebakaran. Penghilangan oksigen ini membahyakan personel dan dapat mematikan. Sangat disarankan digunakan pada fasilitas komputer tanpa awak, atau jika digunakan dalam pusat operasi berawak, sistem pendeteksi api dan alarm harus memungkinkan personel mempunyai cukup waktu untuk keluar ruangan atau membatalkan pelepasan gas CO2. Alat pemadam api portabel biasanya mengandung CO2 atau asam soda dan harus:

a. Ditempatkan di jalan keluar

b. Ditandai dengan tipe apinya

c. Diperiksa oleh personel berlisensi secara teratur

- Halon. Suatu saat Halon pernah dinyatakan sebagai metode pemadaman api yang sempurna pada pusat operasi komputer, berkaitan dengan fakta bahwa zat ini tidak berbahaya bagi peralatan komputer, menyatu dengan baik dengan udara, dan menyembur dengan sangat cepat. Keuntungan menggunakan Halon adalah zat ini tidak meninggalkan bekas residu cair maupun padat. Oleh karena itu, zat ini lebih disukai untuk area yang sensitif, seperti ruangan komputer atau area data storage.

Beberapa masalah muncul dalam pengembangannya, seperti bahwa zat ini tidak boleh dihirup pada konsentrasi lebih dari 10%, dan ketika disemprotkan ke api dengan suhu melebihi 900°F, zat ini terurai menjadi bahan kimia beracun—hidrogen fluorida, hidrogen bromida, dan bromin. Pemakaian pemadam berhalogen dalam ruangan komputer harus dirancang dengan sangat baik, agar memungkinkan personel dievakuasi ketika zat ini dilepaskan baik dari langit-langit maupun dari lantai. Oleh protokol Montreal tahun 1997, Halon dinyatakan sebagai zat yang menipiskan ozon untuk penggunaan senyawa CFC (*chlorofluorocarbon*) olehnya. Halon memiliki potensi merusak ozon yang tinggi (tiga sampai sepuluh kali CFC), dan penggunaanya akan melepas CFC ke lingkungan Tidak ada instalasi Halon 1301 yang dibolehkan, dan instalasi yang telah ada disarankan untuk mengganti Halon dengan bahan yang tidak beracun. Peraturan federal Amerika telah melarang produksi Halon, juga import dan eksport Halon kecuali dengan izin. Ada peraturan yang mengontrol penggunaan, pelepasan, penghapusan wajib Halon.

Ada dua jenis Halon yang digunakan, yaitu:

a. Halon 1211. Bahan uap cair yang digunakan pada pemadam portabel
b. Halon 1301. Bahan bergas yang digunakan dalam sistem *fixed total flooding*

Beberapa bahan pengganti Halon yang dibolehkan oleh EPA:

a. FM-200 (HFC-227ea)

b. CEA-410 atau CEA-308

c. NAF-S-III (HFC Blend A)

d. FE-13 (HFC-23)

e. Argon (IG55) atau Argonite (IG01)

f. Inergen (IG541)

g. Kabut air bertekanan rendah

Kontaminasi dan Kerusakan

Kontaminasi lingkungan akibat kebakaran atau pemadamannya dapat menyebabkan kerusakan pada sistem komputer dengan menimbun partikel penghantar listrik pada komponen. Berikut ini adalah beberapa contoh bahan terkontaminasi akibat kebakaran:

- Asap
- Panas
- Air
- Kontaminasi medium pemadam api (Halon atau CO2).

Tabel berikut menginformasikan suhu yang dibutuhkan untuk merusak berbagai bagian komputer.

Tabel 4. Suhu yang Menyebabkan Kerusakan oleh Panas

Item	Suhu
Hardware komputer	175° F
Storage magnetik	100° F
Produk kertas	350° F

Pemanasan (heating), ventilasi (ventilation), dan AC atau (HVAC)

HVAC terkadang disebut juga HVACR, sebagai tambahan dengan *refrigeration* (pembekuan). Sistem HVAC bisa menjadi sangat rumit dalam gedung-gedung modern yang menjulang tinggi, dan merupakan titik fokus bagi pengendalian lingkungan. Seorang manajer TI harus tahu siapa yang bertanggung jawab atas HVAC, dan langkah-langkah yang jelas harus didefinisikan dengan baik sebelum insiden yang mengancam lingkungan terjadi. Departemen yang sama bertanggung jawab atas api, air, dan potensi bencana lain yang berdampak pada ketersediaan sistem komputer.

2.2.3. Kontrol Fisik dan Teknis

Pada bagian ini, dibahas mengenai elemen keamanan fisik yang dianggap secara spesifik bukan bagian dari solusi administratif, walaupun jelas sekali memiliki aspek administratif. Area yang dicakup adalah kontrol lingkungan, perlindungan kebakaran, daya listrik, penjaga, dan kunci. Elemen-elemen kontrol dibahas sebagaimana kaitannya dengan area kebutuhan kontrol fasilitas, perangkat kontrol akses fasilitas, pendeteksian

penyusupan dan alarm, kontrol invrentori komputer, kebutuhan media storage.

a. Kebutuhan Kontrol Fasilitas

Beberapa elemen dibutuhkan untuk memelihara keamanan fisik atas kontrol fasilitas.

Penjaga

Penjaga merupakan bentuk tertua dari pengawasan keamanan. Penjaga masih memiliki fungsi yang sangat penting dan utama dalam proses keamanan fisik, terutama dalam kontrol garis batas (*perimeter*). Seorang penjaga dapat melakukan sesuatu yang perangkat keras atau perangkat keamanan otomatis lain tidak dapat lakukan karena kemampuannya untuk menyesuaikan diri dengan kondisi yang berubah dengan cepat, belajar dan mengubah pola-pola yang telah dikenali, dan merespon berbagai keadaan di lingkungan.

Penjaga memiliki kemampuan menangkis, merespon, dan mengontrol, sebagai tambahan dari fungsi resepsionis dan pemandu. Penjaga juga merupakan sumber daya terbaik selama periode resiko keselamatan personel karena mereka menjaga perintah, mengendalikan massa, dan evakuasi serta lebih baik dalam pengambilan keputusan ketika terjadi bencana. Mereka cocok ketika keputusan yang segera dan diskrimatif diperlukan oleh entitas keamanan.

Bagaimanapun, penjaga memiliki beberapa kekurangan, seperti:

- Ketersediaan, Mereka tidak dapat hadir dalam lingkungan yang tidak mendukung campur tangan manusia.
- Kehandalan, Seleksi pra kepegawaian penjaga tidak dijamin aman
- Pelatihan, Penjaga bisa ditipu, atau tidak selalu memiliki daftar otorisasi akses yang *up-to-date*.
- Biaya, Memelihara fungsi penjaga dengan menggunakan layanan sendiri atau eksternal memerlukan biaya tinggi.

Anjing

Menggunakan anjing penjaga hampir sama tuanya dengan konsep menggunakan penjaga untuk menjaga sesuatu. Anjing sangat setia, dapat diandalkan, dan memiliki indra pendengaran dan penciuman yang tajam. Anjing penjaga dapat diterima untuk penjagaan fisik garis batas luar (*perimeter*), namun tidak seberguna manusia yang dapat membuat keputusan. Beberapa kelemahan lain termasuk biaya, pemeliharaan, dan masalah asuransi serta pertanggungjawaban.

Pagar

Pemagaran adalah sarana utama untk kontrol akses garis batas luar (*perimeter*) fasilitas. Kategori pemagaran mencakup pagar, gerbang, pintu pagar, dan *mantrap*. Pemagaran dan penghalang lain menyediakan kontrol

kerumunan dan menolong menghalangi penerobosan yang kebetulan dengan mengendalikan akses ke pintu masuk. Kelemahan dari pemagaran adalah biaya, penampilannya (yang mungkin buruk), dan ketidakmampuannya untuk menghentikan penyusup yang gigih. Tabel berikut menunjukan kebutuhan ketinggian pagar.

Tabel 5. Kebutuhan Ketinggian Pagar

Ketinggian	Perlindungan
3 sampai 4 kaki	Menghalangi penerobos yang kebetulan
6 sampai 7 kaki	Sulit didaki dengan mudah
8 kaki dengan 3 untai kawat berduri	Menghalangi penyusup

Mantrap

Mantrap adalah metode kontrol akses fisik dimana pintu masuk diarahkan melalui pintu ganda yang dapat dimonitor oleh penjaga.

Pencahayaan

Pencahayaan juga merupakan bentuk umum dari perlindungan batas. Pencahayaan pelindung yang kuat dan mengarah keluar di pintu masuk dan area parkir dapat menyurutkan pencari dan penyusup. Gedung atau bangunan yang terproteksi dengan kritis harus disinari sampai ketinggian 8 kaki. Tipe-tipe umum pencahayaan mencakup *floodlight*, lampu jalan, *fresnel light*, dan lampu pencari.

Kunci

Setelah menggunakan penjaga, kunci mungkin menjadi salah satu metode kontrol akses yang pernah digunakan. Kunci dapat dibagi menjadi dua jenis: *preset* dan yang dapat diprogram (*programmable*)

- Kunci *Preset*.

Ini adalah kunci pintu pada umumnya. Kombinasi untuk membuka tidak dapat diubah kecuali dengan menghilangkannya secara fisik dan mengganti mekanisme internalnya. Ada beberapa variasi kunci *preset*, termasuk *key-in-knob*, *mortise*, dan *rim lock*. Semua ini terdiri dari berbagai gerendel, silinder, dan selot.

- Kunci *Programmable*.

Kunci ini bisa berbasis mekanik ataupun elektronik. Kunci *programmable* yang mekanik sering berupa kunci putar kombinasi, seperti yang digunakan pada loker di arena olahraga. Jenis lain dari kunci *programmable* yang mekanik adalah kunci tombol lima-angka yang membutuhkan pengguna untuk memasukkan kombinasi angka. Kunci ini sangat populer untuk pusat operasi TI.

Kunci *programmable* yang elektronik membutuhkan pengguna untuk memasukkan pola angka digit pada *keypad* numerik, dan mungkin menampilkan digit secara random setiap kalinya untuk mencegah pengintip pola input. Ini juga dikenal sebagai kunci sandi atau kontrol akses *keypad*.

CCTV (*Closed-Circuit Television*)

Pengawasan visual atau perangkat perekam seperti CCTV digunakan sebagai tambahan penjaga untuk meningkatkan kemampuan pengawasan dan merekam peristiwa untuk analisis di masa depan atau untuk kepentingan bukti kejahatan dan penuntutan. Perangkat ini bisa berupa fotografik seperti kamera foto atau kamera video, atau elektronik seperti kamera CCTV. CCTV dapat digunakan untuk memonitor peristiwa langsung yang terjadi di daerah yang jauh dari jangkauan penjaga, atau dapat digunakan bersama VCR sebagai metode yang efektif dalam biaya untuk merekam peristiwa.

Perlu diingat, bahwa memonitor peristiwa adalah tindakan pencegahan, dan merekam peristiwa dianggap sebagai tindakan pendeteksian.

b. Perangkat Kontrol Akses Fasilitas

Akses ini mencakup kontrol akses personel terhadap fasilitas dan pusat operasi yang umum, sebagai tambahan kontrol akses *data center* yang spesifik. Hal yang berkaitan dengan pengendalian akses fisik berikut merupakan sebagian dari beberapa faktor otentikasi. Ada tiga faktor yang berkaitan dengan otentikasi: 1. sesuatu yang Anda punya (*something you have*) seperti kartu pengenal, 2. sesuatu yang anda tahu (*something you know*),

seperti PIN atau *password,* dan 3. Siapa diri anda (*something you are*) seperti biometrik.

Kartu Akses Keamanan (*Security Access Card*)

Kartu akses keamanan adalah metode umum dalam kontrol akses fisik. Ada dua tipe umum kartu—kartu gambar foto dan kartu bersandi digital. Kedua grup kartu ini juga disebut sebagai kartu bodoh (*dumb card*) dan kartu pintar (*smart card*). Kartu bodoh membutuhkan penjaga untuk membuat keputusan mengenai keabsahannya, sementara kartu pintar membuat keputusan masuk secara elektronik.

- Kartu berfoto (*Photo-Image Card*). Kartu berfoto adalah kartu identifikasi yang sederhana dengan adanya foto pemegang kartu sebagai alat identifikasinya. Ini adalah kartu ID standar yang berfoto, seperti kartu SIM ataupun kartu pegawai. Kartu ini disebut bodoh karena tidak mempunyai kecerdasan di dalamnya, dan perlu dibuat keputusan aktif oleh personel di pintu masuk sebagai otentikasi
- Kartu Sandi Digital (*Digital-Coded Card*). Kartu sandi digital mengandung chip atau sandi garis magnetik (sebagai tambahan atas foto pemegang kartu). Pembaca kartu dapat diprogram untuk menerima akses berdasarkan komputer kontrol akses online yang juga menyediakan informasi mengenai tanggal dan waktu akses masuk. Kartu jenis ini juga bisa membuat pengelompokan akses banyak tingkat.

Ada dua bentuk umum kartu sandi digital, yaitu *smart card* dan *smarter card*. Kartu *smart card* memiliki kode garis magnetik atau chip IC (*Integrated Circuit*) kecil yang tertanam di dalamnya. Penggunaan kartu ini membutuhkan pengetahuan *password* atau PIN (*Personal Identification Number*) untuk mendapat akses masuk. Kartu ATM adalah contoh dari kartu model ini. Kartu ini mengandung prosesor tersandikan dengan protokol otentikasi sistem, ruang memori *read-only* untuk program dan data, dan beberapa diantaranya dilengkapi dengan sejenis antarmuka pengguna (*user interface*).

Dalam beberapa skenario kartu *smart card* dapat dipasangkan dengan token otentikasi yang membangkitkan *password* atau PIN yang sekali pakai (one-time) atau berupa *challenge-response*. Sementara otentikasi *dual-factor* paling banyak digunakan untuk akses logik layanan jaringan, kartu *smart card* bisa dikombinasikan dengan *card reader* yang pintar untuk menyediakan kontrol yang sangat kuat terhadap akses fasilitas.

- *Wireless Proximity Reader*. *Proximity reader* tidak membutuhkan pengguna untuk memasukkan kartu. Kartu ini juga biasa disebut sebagai *wireless security card*. *Card reader* mengindra kartu milik pengguna di area umum pada jarak atau kedekatan tertentu dan membolehkan akses. Ada dua tipe umum *proximity reader*—yang diaktifasi oleh pengguna (*user activated*) atau yang mendeteksi sistem (*system sensing*). *Proximity card* yang diaktifasi pengguna memancarkan urutan input masukan ke *wireless keypad* pada *reader*. *Keypad* pada *reader* mengandung pola kode unik yang

permanen maupun yang dapat diprogram. *Proximity card* yang mendeteksi sistem mengenali kehadiran perangkat bersandi dalam area umum *reader*. Berikut ini adalah tiga tipe umum kartu yang mendeteksi sistem, yang didasarkan pada cara daya listrik dibangkitkan pada perangkatnya:

- *Passive device*. Kartu ini tidak mengandung baterai, namun mengindra medan elektromagnet yang dipancarkan oleh reader dan memancarkan frekuensi berbeda menggunakan medan daya dari *reader*.
- *Field Powered device*. Mengandung elektronik aktif, pemancar frekuensi radio, dan sirkuit catu daya pada kartu.
- *Transponder*. Baik kartu maupun *reader* mengandung penerima sinyal (*receiver*), pemancar, elektronik aktif, dan baterai. *Reader* memancarkan sinyal interogasi pada kartu, yang menyebabkan kartu memancarkan kode akses. Sistem ini sering digunakan sebagai alat portabel untuk memberikan kontrol akses secara dinamik. Tabel di bawah mendaftarkan berbagai tipe kartu *security access*

Tabel 6. Tipe Kartu *Security Access*

Tipe Kartu	Keterangan
Foto ID	Terdapat gambar foto wajah
Optical-coded	Terdapat kisi-kisi pola titik digital yang dibuat dengan laser
Electric circuit	IC yang dicetak pada kartu
Magnetic Stripe	Garis-garis dari bahan magnetik
Magnetic Strip	Sederetan carik tembaga
Passive electronic	Sirkuit listrik frekuensi radio
Active electronic	Lencana yang memancarkan kode elektronik

Perangkat *Biometric*

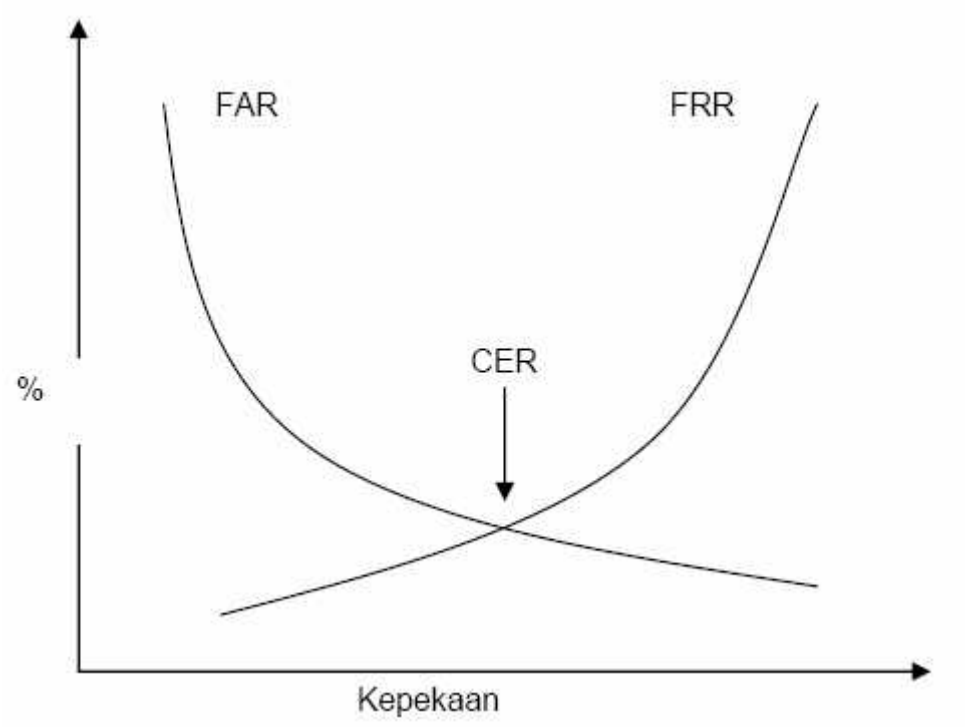
Alternatif lain dari penggunaan password atau kartu identitas dalam kontrol akses secara lojik maupun teknis adalah biometrik. Biometrik didasarkan pada faktor atau tipe ketiga dalam mekanisme otentikasi : siapa diri Anda (*something you are*). Biometrik didefinisikan sebagai alat otomasi untuk mengidentifikasi dan mengotentikasi identitas seseorang berdasarkan ciri-ciri fisiologis atau kebiasaan. Dalam biometrik, identifikasi adalah pencarian dari satu-ke-banyak dari karakteristik individu dalam basisdata.

Otentikasi dalam biometrik adalah pencarian dari satu-ke-satu untuk memverifikasi pengakuan identitas yang dilakukan seseorang. Biometrik digunakan untuk identifikasi dalam kontrol fisik, dan untuk otentikasi dalam kontrol lojik. Ada tiga ukuran kinerja dalam biometrik:

1. *False Rejection Rate (FRR)* atau error tipe I. Persentase subjek valid yang ditolak secara salah
2. *False Acceptance Rate (FAR)* atau error tipe II. Persentase subjek tidak valid yang diterima secara salah.
3. *Crossover Error Rate (CRR)*. Persen dimana nilai FRR sama dengan nilai FAR.

Hampir semua tipe deteksi membolehkan kepekaan sistem untuk ditingkatkan atau diturunkan selama proses inpeksi. Jika kepekaan sistem

ditingkatkan, seperti detektor metal di bandar udara, sistem menjadi sangat selektif dan memiliki nilai FRR yang tinggi. Sebaliknya, jika kepekaan diturunkan, nilai FAR akan naik. Jadi, untuk memiliki ukuran yang tepat dari kinerja biometrik CER digunakan sebagaimana yang tergambar pada gambar di bawah ini.



Gambar 1. *Crossover Error Rate* (CER)

Sebagai tambahan akurasi sistem biometrik, ada beberapa faktor yang harus diperhatikan. Faktor ini mencakup *enrollment time*, tingkat *throughput*, dan akseptabilitas. *Enrollment time* adalah waktu yang dibutuhkan untuk mendaftarkan pada sistem dengan menyediakan sampel ciri-ciri biometrik

untuk dievaluasi. *Enrollment time* yang diterima adalah sekitar dua menit. Sebagai contoh, dalam sistem sidik jari, sidik jari aktual disimpan membutuhkan sekitar 250KB per jari untuk gambar berkualitas tinggi. Tingkat informasi seperti ini dibutuhkan dalam pencarian dari satu-ke-banyak oleh aplikasi forensik pada basisdata yang sangat besar. Dalam teknologi pindai jari (*finger scan*), sidik jari penuh tidak disimpan, melainkan ciri yang diekstrak dari sidik jari disimpan menggunakan *template* kecil yang membutuhkan kira-kira 500 sampai 1000 byte ruang penyimpanan. Teknologi *finger scan* digunakan untuk verifikasi satu-ke-satu dengan menggunakan basisdata yang lebih kecil. Pembaruan (*update*) dari informasi *enrollment* dibutuhkan karena beberapa ciri biometrik, seperti suara dan tandatangan, boleh jadi berubah seiring berjalannya waktu.

Tingkat *throughput* adalah kecepatan dimana sistem memproses dan mengidentifikasi atau mengotentikasi individu. Tingkat kecepatan throughput yang dapat diterima adalah 10 subyek per menit. Akseptabilitas mengacu pada pertimbangan privasi, dan kenyamanan fisik dan psikologis ketika menggunakan sistem. Sebagai contoh, masalah pada pindai retina (*retina scan*) bisa berupa pertukaran cairan tubuh pada bola mata.

Masalah lain yang mungkin terjadi adalah pola retina bisa menunjukkan kondisi kesehatan seseorang, seperti menderita diabetes atau

tekanan darah tinggi. Gambar atau citra biometrik disimpan pada seuatu area yang disebut sebagai *corpus*. *Corpus* disimpan pada sebuah basisdata gambar. Sumber kesalahan yang potensial adalah perubahan pada gambar selama pengumpulan dan kesalahan memberi label atau masalah penulisan lain yang berhubungan dengan basisdata. Oleh karena itu, proses pengumpulan gambar dan penyimpanannya harus dilakukan dengan cermat melalui pengecekan.

Pendeteksian Penyusupan dan Alarm

Pendeteksian penyusup mengacu pada proses identifikasi usaha masuk ke dalam sistem atau gedung untuk memperoleh akses tak berwenang. Sementara pada Bab 3 dijelaskan dengan detil sistem identifikasi yang mendeteksi pelanggaran lojik pada infrastruktur jaringan, di Bab ini dibicarakan mengenai perangkat yang mendeteksi pelanggaran fisik dari keamanan batas area, seperti alarm pencuri.

2.2.4. Kontrol Inventori Komputer

Kontrol inventori komputer adalah kontrol terhadap komputer dan peralatan komputer dari pencurian fisik dan perlindungan terhadap kerusakan. Dua area perhatian utama adalah kontrol fisik komputer dan kontrol laptop.

a. Kontrol Fisik Komputer

Berkaitan dengan perkembangan komputasi tersebar dan perkembangan laptop, kontrol inventori pada level mikrokomputer adalah masalah besar. Beberapa kelompok memperkirakan bahwa 40% penyusutan inventori komputer disebabkan oleh hilangnya komponen-komponen mikrokomputer. Beberapa kontrol fisik harus diambil untuk meminimalkan kerugian ini:

Kunci Kabel. Kunci kabel terdiri dari kabel baja berselaput vinyl yang menempelkan komputer atau periferal pada meja. Kabel ini sering terdiri dari obeng (*screw kit*), kunci celah (*slot lock*), dan perangkap kabel (*cable trap*).

Kontrol Port *(Port Control)*. *Port control* adalah alat yang mengamankan port data (seperti *floppy drive* atau port serial atau pararel) dan mencegah penggunaannya.

Kontrol Saklar *(Switch Control)*. Sebuah *switch control* adalah penutup dari saklar on/off, yang mencegah pengguna mematikan daya listrik dari server file.

Kontrol Saklar Periferal *(Peripheral Switch Control)*. Kontrol tipe ini adalah saklar yang dapat dikunci yang mencegah penggunaan *keyboard*.

Electronic Security Board. Papan ini dimasukkan pada slot tambahan pada komputer dan memaksa pengguna untuk memasukkan *password* ketika

komputer dinyalakan. Ini juga merupakan bagian standar dari BIOS (*Basic Input Output System*) dari komputer-komputer yang tersedia di pasaran. Ini juga biasa disebut kunci kriptografik.

b. Kontrol Laptop

Perkembangan jumlah laptop dan perangkat portabel adalah evolusi berikutnya dari komputasi tersebar dan meningkatkan tantangan bagi praktisi keamanan. Sekarang sumber daya komputer bertebaran di seluruh dunia., dan kontrol inventori fisik hampir tidak mungkin dilakukan oleh organisasi. Pencurian laptop adalah masalah serius kerena mengakibatkan kegagalan dalam ketiga elemen C.I.A: *Confidentiality* (kerahasiaan), karena data pada laptop dapat dibaca oleh seseorang di luar lingkungan yang termonitor; *Availability* (ketersediaan) karena pengguna telah kehilangan unit komputasi; dan *Integrity* (Keutuhan) karena data yang ada di dalamnya dan telekomunikasi darinya dapat dicurigai tidak otentik dan tidak utuh lagi.

c. Kebutuhan Media Storage

Penyimpanan data media serta pembuangan media dan laporan yang sudah tidak digunakan adalah masalah serius bagi praktisi keamanan. Kadangkala organisasi akan mencurahkan sejumlah besar sumber daya untuk perlindungan perimeter dan keamanan jaringan, dan akan membuang dokumen laporan secara tidak layak. Atau juga, mereka terbiasa

menggunakan ulang laptop atau disket tanpa benar-benar menghapus data yang telah ada sebelumnya.

Oleh karena pencurian laptop kian merajalela, enkripsi data yang sensitif pada perangkat portabel menjadi kebutuhan mutlak. Pernah terjadi kasus dimana seseorang telah dipinjami sebuah laptop ketika bekerja pada perusahan broker saham top, dan ia menemukan bahwa *hard drive*-nya belum diformat. *Hard drive* itu mengandung banyak data email sensitif mengenai pemilihan presiden Amerika Serikat pada tahun 1996.

2.3. Tren Teknologi Keamanan Fisik

Face recognizer

Face recognizer merupakan pengembangan lebih lanjut dari *face scanner*. Pada *face recognizer* wajah dikenali berdasarkan data struktur muka dan tidak lagi mencocokan gambar atau bentuk muka. Data struktur muka ini bisa terdiri dari jarak antar mata, bentuk mata, panjang hidung, jarak antara pipi dan dagu, dan sebagainya sehingga diharapkan bisa lebih sahih /tepat dalam mengidentifikasi dibanding *face scanner*.

Face recognizer lebih fleksibel digunakan karena hanya membutuhkan data berupa gambar atau foto wajah untuk registrasi maupun identifikasi serta tidak perlu melakukan pemindaian (*scanning*) wajah yang memakan

waktu lebih lama dan membutuhkan kerelaan orang yang akan dipindai wajahnya. Perangkat ini sudah diterapkan di beberapa bandara internasional untuk mencekal penjahat dan di beberapa stadion untuk mencekal para perusuh pertandingan sepak bola (*hooligans*)

Anti passback

Anti passback adalah cara untuk mencegah kembalinya tanda identitas otorisasi ke belakang untuk diberikan kepada orang lain. Anti passback dapat dilakukan dengan pemasangan pintu satu arah yang hanya bisa dibuka dari satu sisi. Pengecekan di banyak checkpoint juga dapat dilakukan agar pemegang kartu selalu membutuhkan kartunya di setiap *checkpoint.*

Mantrap

Mantrap adalah perangkat keamanan kontrol akses fisik untuk mencegah otorisasi izin masuk bagi seseorang digunakan lebih dari satu orang. Mantrap juga akan mencegah adanya pengekor yang memanfaatkan akses orang yang sah terotorisasi dengan cara mengikutinya diam-diam di belakangnya. Perangkat mantrap biasanya berupa sebuah kompartemen tertutup yang hanya bisa dimasuki oleh satu orang. Di kompartemen itulah dilakukan pengecekan otorisasi untuk memperoleh hak akses memasuki area keamanan.

Keep in

Keep (the thief) in adalah salah satu metoda penanggulangan pencurian. Selama ini, metoda keamanan yang lazim adalah dengan *keep out* yang mencegah pencuri agar tidak dapat masuk ke area keamanan. Ada kalanya pencuri berhasil menaklukan sistem keamanan model seperti ini dan terus melakukan kejahatannya. *Keep the thief in* merupakan metoda tambahan terhadap cara *keep the thief out* dengan cara mencegah pencuri keluar area keamanan setelah terjadinya kejahatan.

Contoh cara dan perangkat metoda ini adalah sistem kerangkeng. Begitu terjadi peristiwa pencurian setelah pencuri berhasil menaklukan sistem pencegahan pencurian, selain akan membangkitkan alarm, sistem juga akan mengaktifkan kerangkeng di area keamanan. Kerangkeng ini akan mengurung pencuri di tempat kejadian sehingga ia tidak dapat kabur dan melarikan barang curiannya. Perangkat ini biasanya digunakan di tempat keamanan yang banyak diakses publik seperti museum. Museum Louvre di Paris Perancis adalah salah satunya.

Integrasi keamanan fisik dengan TI

OSE (*Open Security Exchange*) adalah badan yang mempelopori upaya integrasi antara perangkat keamanan fisik dengan sistem komputer organisasi. OSE merupakan badan kolaborasi antara beberapa perusahaan

yang bertujuan untuk menciptakan standar desain spesifikasi interoperabilitas yang memungkinkan beberapa perangkat keamanan dapat berkomunikasi dan berinteroperasi Model standar seperti ini berguna menjembatani kedua area. Sebagai contoh, selama ini belum ada korelasi langsung antara TI dengan perangkat *anti-passback* sebagai kontrol akses fisik Model standar dan spesifikasi ini juga akan memberikan para profesional keamanan kemampuan untuk mengontrol dan memonitor even keamanan dengan cara yang lebih terpusat daripada melakukannya dengan pelacakan terhadap banyak sistem yang terpisah dan independen.

BAB III

PEMBAHASAN

Menurut departemen koperasi dan usaha kecil menengah, UKM adalah usaha yang memiliki kekayaan bersih paling banyak sebesar dua ratus juta rupiah di luar tanah dan bangunan tempat usaha, dan memiliki hasil penjualan tahunan paling banyak satu milyar rupiah. Ditinjuau dari aspek penggunaan TI, UKM bisa jadi belum menerapkan komputerisasi dalam mendukung aktivitas organisasinya, sudah terkomputerisasi namun tidak terintegrasi, atau sudah terkomputerisasi yang terintegrasi. UKM yang sudah sadar TI lazimnya memiliki sistem komputer untuk mendukung kegiatan operasionalnya, dan mengorganisasi data operasionalnya pada sebuah data center sederhana. Tenaga terdidik dan terlatih TI yang dipekerjakan UKM berkisar antara 0 sampai 5 orang.

3.1. Kontrol Administratif

3.1.1. Perencanaan Kebutuhan Fasilitas

Pemilihan site

Jika UKM mengelola sistem pemrosesan transaksi dan data center yang *standalone* atau terkoneksi dalam sebuah jaringan lokal, kantor UKM harus memiliki keamanan fisik yang baik untuk perlindungan terhadap

sistem komputer maupun aset berharga lain yang dimiliki organisasi. Mula-mula harus dipikirkan tentang pemilihan lokasi dimana sistem komputer ditempatkan dan dioperasikan. Semua syarat pemilihan lokasi yang telah disebutkan dalam teori harus dipenuhi baik untuk bangunan kantor milik sendiri atau berlokasi di gedung perkantoran bersama. Syarat ini meliputi:

- Visibilitas

Visibilitas yang rendah adalah keharusan. Hal ini diperlukan agar sistem komputer tidak menarik atau memancing perhatian orang yang berniat buruk.

- Pertimbangan Lingkungan Sosial Lokasi

Pilihlah lokasi yang memiliki tingkat kriminalitas rendah, jauh dari tempat pembuangan sampah, jauh dari sumber bahaya dan indikasi lingkungan sosial lain yang buruk.

- Bencana Alam

Pastikan memilih lokasi yang bersiko rendah terhadap bencana alam. Cari tahu lebih lanjut informasi tentang banjir, angin, resiko kebakaran serta kemungkinan terjadnya gempa bumi di lokasi yang direncanakan.

- Transportasi

Lokasi yang cukup jauh dari masalah akibat lalu lintas darat, laut ataupun udara yang berlebihan sangat disukai. Masalah ini bisa jadi

kemacetan, tingkat kecelakaan yang tinggi, atau lokasi yang terlalu dekat dengan pelabuhan atau bandara yang sibuk. Hal ini diperlukan untuk mencegah terhambatnya tindakan pertolongan oleh layanan eksternal (polisi, pemadam kebakaran, ambulans) ketika terjadi peristiwa ancaman keamanan fisik.

- Tanggungjawab bersama

Adanya tanggungjawab bersama terhadap kontrol lingkungan atau HVAC (*heating, ventilation and air conditioning*) harus diperhatikan. Perjelas batasan dan akses terhadap fasilitas bersama tersebut. Sebuah data center tidak boleh memiliki akses penuh ke sistem ketika keadaan emergensi terjadi.

- Layanan Eksternal

Sangat disarankan lokasi yang direncanakan berada dalam jangkauan layanan gawat darurat, kantor polisi, kebakaran, dan rumah sakit atau fasilitas medis yang dekat sehingga cepat dalam mengantisipasi kejadian.

Untuk UKM dengan dengan sistem pemrosesan transaksi dan data center yang terhubung ke internet, sebaiknya UKM menempatkan mesin server aplikasi dan server basisdata milik sendiri pada sebuah provider koneksi layanan internet. Salah satu pilihan yang bisa diambil adalah dengan melakukan *colocation* di IDC (Indonesia Data Center) di gedung Cyber, Jakarta. Provider yang menyediakan layanan co-location biasanya sudah memiliki layanan dan infrastruktur keamanan fisik yang sudah layak

sehingga tidak perlu dipikirkan lagi oleh UKM. Pilihan melakukan penempatan aplikasi dan basisdata dengan hosting tidak dianjurkan, mengingat kita tidak mengetahui tingkat kredibilitas perusahaan yang menyediakan layanan hosting sehingga tidak ada jaminan keamanan data dan transaksi bagi perusahaan UKM.

Perancangan site

Bagi UKM yang memutuskan untuk memelihara site sistem pemrosesan transaksi operasional atau data center secara mandiri, perusahaan harus memikirkan perancangan pembangunan site yang aman bagi sistem komputer mereka. Hal yang menjadi perlu menjadi perhatian selama tahap perencanaan pembangunan *site* adalah seperti dijabarkan di bawah ini:

- Tembok

Keseluruhan tembok, dari lantai hingga langit-langit, harus memiliki standar keamanan terhadap kebakaran yang cukup. Lemari atau ruangan yang dijadikan tempat penyimpanan media harus memiliki standar yang tinggi pula, yaitu tahan api.

- Langit-langit

Untuk bangunan bertingkat masalah yang dipertimbangkan adalah standar kemampuan menahan beban. Di luar itu standar keamanan dan

ketahanan terhadap kebakaran juga menjadi permasalahan bersama berbagai jenis bangunan. Hindari penggunaan bahan yang mudah terbakar atau bahan beracun seperti asbes. Langit-langit juga biasa digunakan sebagai akses masuk bagi pencuri. Perkecil resiko terjadinya penyusupan melalui langit-langit dengan membuat langitlangit yang tebal dan tidak mudah dibuka atau dibongkar.

- Lantai

Lantai harus memiliki kemampuan menahan beban yang memadai, khususnya untuk bangunan bertingkat. Tidak hanya pada keadaan biasa, kemampuan lebih diperlukan untuk menahan beban bangunan agar tidak runtuh ketika terjadi kebakaran. Bahan yang kuat dan tahan api mutlak diperlukan. Hal ini perlu diperhatikan karena banyak terjadi kasus daya dukung struktur sebuah bangunan menjadi lemah ketika terjadi peningkatan suhu akibat kebakaran. Oleh karena itu pondasi lantai bangunan bertingkat, apapun bentuknya, harus terbuat dari beton, bukan frame kayu atau frame logam.

- Jendela

Sebuah ruangan sistem komputer berupa data center boleh tidak memiliki jendela. Tapi jika ingin ada jendela, buatlah jendela yang tembus cahaya (bukan tembus pandang) dan anti pecah.

- Pintu

Pintu bangunan harus tahan terhadap pembobolan, dan memiliki ketahanan terhadap api yang sama seperti pada tembok. Jalan keluar atau akses keluarmasuk harus diawasi, minimal oleh penjaga atau alarm. Pintu elektrik dinilai tidak terlalu perlu untuk beberapa UKM, terutama untuk UKM-UKM skala kecil karena harga pintu elektrik cukup mahal, dan bisa digantikan dengan alternatif lain yang lebih sederhana dan terjangkau, yaitu penjaga atau alarm.

- Pemancar Air

Pemancar air merupakan perangkat keamanan fisik yang handal untuk menanggulangi terjadinya kebakaran. Akan tetapi, untuk mengimplementasikan pemancar air membutuhkan biaya cukup banyak. Hal ini akan memberatkan bagi UKM. Penyediaan fire extinguiher dapat menggantikan pemancar air. Agar optimal, fire extinguisher harus ditempatkan di beberapa tempat, dan perlu komitmen untuk melakukan kontrol berkala.

- Jaringan pipa dan gas

Jika bangunan memiliki jaringan pipa, gas atau saluran AC, harus dipastikan jaringan tersebut dirancang dan dipasang atau ditanam dengan aman. Akan lebih baik pula jika dilakukan prosedur pengecekan dan pemeliharaan berkala.

- AC

Sumber daya listrik untuk AC harus disediakan khusus dengan EPO (Emergency Power Off)-nya jika UKM membutuhkan dukungan reliabilitas tinggi dari sistem komputer pada saat daya listrik turun. Untuk perangkat komputer yang menurut penilaian UKM sangat kritis dan sensitif, AC harus bisa menyediakan kestabilan suhu, dan kelembapan. Tekanan udara positif dari AC juga dibutuhkan jika ingin melindungi komputer dari debu.

- Kebutuhan Kelistrikan.

Jika memiliki anggaran berlebih, UKM sebaiknya memiliki fasilitas sumber daya listrik cadangan yang layak. Jika tidak, UKM harus membentengi pasokan daya listrik pada perangkat sistem komputernya dengan stabilizer dan UPS (Uninterruptable Power Supply).

b. Manajemen Keamanan Fasilitas

Jejak Audit

Model jejak audit yang cocok untuk diterapkan oleh UKM sebagai salah satu bentuk perlingunan fisik terhadap sistem komputernya adalah berupa:

- pencatatan log pengunjung ruang komputer
- pencatatan log pemakaian komputer yang dilakukan oleh sistem software dengan mengaktifkan fitur otentikasi dan mode multiuser untuk melindungi informasi yang ada dalam komputer.

Untuk UKM, informasi yang dicatat dalam log sudah mencukupi jika mencakup tanggal akses

- tempat akses
- pelaku akses
- status akses

Untuk itu agar dapat melakukan pengontrolan akses, perlu didefinisikan terlebih dahulu model physical access control list-nya. Model dan pencatatan log ini diusahakan dibuat sesederhana mungkin sehingga jejak audit dapat menolong seorang administrator merekonstruksi detail penyusupan setelah kejadian.

Prosedur Emergensi

Semua elemen administrasi prosedur emergensi yang mencakup hal berikut:

- Prosedur shutdown sistem darurat
- Prosedur evakuasi sederhana
- Pelatihan pegawai, pendalaman pengetahuan secara periodik
- Testing sistem dan peralatan secara periodik harus dimiliki pula oleh organisasi UKM.

Prosedur-prosedur ini harus didokumentasikan dengan jelas, siap akses (termasuk salinan yang disimpan di tempat lain pada kejadian

bencana), dan di-update secara periodik. Terlebih dari semua itu, hal yang paling utama adalah komitmen organisasi untuk melaksanakannya.dengan konsisten.

Kontrol personel administratif

Kontrol personel administratif yang dapat diterapkan oleh UKM adalah sebagai berikut:

- Screening pra kepegawaian:

Cukup hanya pengecekan sejarah kepegawaian, pendidikan, dan referensi. Penyelidikan latar belakang atau penghargaan untuk posisi yang penting dan sensitif tidak terlalu dibutuhkan.

- Pengawasan kepegawaian

Kejelasan tingkat keamanan yang dibuat jika pegawai memiliki akses ke dokumen rahasia. Penilaian atau review pegawai oleh penyelia mereka tidak diperlukan namun cukup pengawasan atau monitoring atas pegawai saja

- Prosedur pasca kepegawaian

Prosedur wawancara ketika pegawai keluar tidak perlu dilakukan namun penghapusan akses ke jaringan dan penggantian password adalah suatu keharusan. Lakukan juga pengembalian inventaris komputer, laptop, atau item lain jika dipinjamkan ke pegawai.

3.2. Kontrol Lingkungan dan Keselamatan Hidup

Daya Listrik

Dalam kaitannya dengan daya listrik, gangguan yang mungkin terjadi adalah berupa gangguan ketidakstabilan listrik, interferensi gelombang radio dan elektromagnetik, dan listrik statis. Gangguan ketidakstabilan daya listrik dapat ditanggulangi secara murah dengan penggunaan UPS (*Uninterruptable Power Supply*) dan stabilizer. Penempatan (*positioning*) barang-barang elektronik yang baik dapat mengurangi gangguan interferensi gelombang radio dan elektromagnetik Solusi murah untuk gangguan listrik statis dilakukan dengan:

- menyemprotkan spray anti listrik statik pada lantai, meja dan peralatan elektronik
- gedung, dan ruangan komputer harus di-ground dengan baik mengendalikan tingkat kelembapan ruangan berkomputer dengan AC.
- Solusi di bawah ini dinilai kurang cocok diterapkan pada UKM dengan pertimbangan biaya dan tingkat urgensinya yang rendah karena ada alternatif lain seperti di atas yang dipandang lebih ekonomis.
- penggunaan lantai anti listrik statik pada ruangan pusat operasi atau pusat komputer.
- penggunaan meja atau karpet anti listrik statik.

Pendeteksian dan Pemadaman Kebakaran

- detektor api

Kebutuhan UKM akan perangkat pendeteksi api tidak terlalu penting. UKM biasanya menempati gedung atau bangunan yang tidak terlalu besar sehingga keberadaan api dapt dengan mudah langsung diketahui dan dilihat. Pada kenyataanya, kebanyakan kasus kebakaran justru disebabkan oleh kesalahan manusia (human error) seperti korsleting, ledakan kompor, atau rokok.

Kejadian pemicu api jenis tersebut mudah dideteksi pada bangunan yang kecil dan ditempati manusia. Namun jika tetap ingin menggunakan detektor api, pilihan jenis detektor yang tepat bagi UKM adalah detektor api pendeteksi panas

- Sistem pemadam kebakaran : pipa kering, pipa basah,

Sistem pemadam kebakaran berupa pemancar air menghabiskan investasi yang cukup besar sehingga tidak disarankan untuk UKM.

- Pemadam api (*fire extinguisher*)

Seperti yang telah disebutkan di atas fire extinguisher dapat menggantikan keberadaan sistem pemancar air. Fire extinguisher perlu ditempatkan di beberapa lokasi dan dicek secara berkala agar selalu siap digunakan. Fire extinguisher yang hampir atau sudah kadaluarsa dapat dimanfaatkan sebagai alat bantu dan sarana pelatihan pemadaman api.

3.3. Kontrol Fisik dan Teknis

Kebutuhan Kontrol Fasilitas

Beberapa elemen yang cocok bagi UKM untuk memelihara keamanan fisik atas kontrol fasilitas sistem komputer adalah:

- Penjaga

Untuk menjamin kehandalan, perlu dilakukan seleksi pada saat perekrutan dan pelatihan. Penugasan penjaga dalam beberapa shift waktu kerja dapat menjamin ketersediaan kapan saja, sebagaimana pula kehandalan.

- Pagar

Pagar dengan ketinggian yang memadai diperlukan menghalangi penerobos dan penyusup.

- Pencahayaan

Pencahayaan mutlak diperlukan sebagai elemen perlindungan tambahan selain penjaga dan pagar terutama di malam hari

- Kunci

Kunci preset lebih disarankan daripada kunci yang programmable untuk alasan biaya. Penggunaan anjing dan CCTV dinilai tidak ekonomis bagi UKM.

Perangkat Kontrol Fasilitas

Dua perangkat kontrol akses fisik terhadap fasilitas adalah kartu akses dan perangkat biometrik. Dari berbagai jenis kartu akses yang telah

dijelaskan pada bagian teori, jenis kartu yang cocok bagi UKM adalah kartu akses berfoto. Kartu sandi digital dan kartu *wireless* tidak cocok digunakan karena membutuhkan perangkat tambahan yang tidak murah. Begitu pula halnya dengan perangkat biometrik.

Pendeteksi Penyusup dan Alarm

Segala bentuk detektor penyusup dan detektor gerak dinilai berlebihan untuk diterapkan pada industri UKM. Sistem alarm pun demikian, kecuali untuk sistem alarm manual, yaitu yang diaktifkan dengan menekan tombol secara manual, dan yang bukan dipicu oleh sinyal dari perangkat pendeteksi penyusup atau pendeteksi gerak.

3.4. Kontrol Inventori Komputer

Kontrol Fisik Komputer

Kontrol fisik komputer bertujuan mencegah perangkat komputer dari pecurian. Beberapa kontrol fisik harus diambil untuk meminimalkan kerugian ini:

- Kunci Kabel. Kunci kabel terdiri dari kabel baja berselaput vinyl yang menempelkan komputer atau periferal pada meja. Kabel ini sering terdiri dari obeng (screw kit), kunci celah (slot lock), dan perangkap kabel (cable trap).

- Kontrol Port (Port Control). Port control adalah alat yang mengamankan port data (seperti floppy drive atau port serial atau pararel) dan mencegah penggunaannya.
- Kontrol Saklar (Switch Control). Sebuah switch control adalah penutup dari saklar on/off, yang mencegah pengguna mematikan daya listrik dari server file.
- Kontrol Saklar Periferal (Peripheral Switch Control). Kontrol tipe ini adalah saklar yang dapat dikunci yang mencegah penggunaan keyboard.
- Electronic *Security Board*. Papan ini dimasukkan pada slot tambahan pada komputer dan memaksa pengguna untuk memasukkan *password* ketika komputer dinyalakan. Ini juga merupakan bagian standar dari BIOS (*Basic Input Output System*) dari komputer-komputer yang tersedia di pasaran. Ini juga biasa disebut kunci kriptografik.

Semua kontrol diatas cocok untuk digunakan oleh UKM karena harganya yang tidak mahal, namun tidak perlu diterapkan semuanya tapi bergantung pada kebutuhaannya.

Kontrol Laptop

Kontrol laptop yang bisa dilakukan dengan murah adalah dengan memberi kunci pada port daya listrik laptop. Kunci ini akan mencegah pencuri mengambil laptop, setidaknya ia harus berusaha mencabut kabel

dayanya yang tertancap di tembok. Oleh karena itu UKM disarankan agar memiliki colokan listrik yang tersembunyi.

Kebutuhan Media Storage

UKM sebaiknya mengetahui dan menginventarisi atau mengontrol media-media yang memungkinkan terjadinya kehilangan dan kebocoran data. Pada bagian pembahasan teori telah diketahui bahwa media ini termasuk*atape* untuk *backup* data, CD, disket, *Hard driv,* dan kertas hasil *printout* atau berkas laporan baik pada *on-site* maupun *off-site*.

BAB IV

PENUTUP

Jika UKM mengelola sistem pemrosesan transaksi dan data center yang *standalone* atau terkoneksi dalam sebuah jaringan lokal, kantor UKM harus memiliki keamanan fisik yang baik untuk perlindungan terhadap sistem komputer maupun aset berharga lain yang dimiliki organisasi. Mula-mula harus dipikirkan tentang pemilihan lokasi dimana sistem komputer ditempatkan dan dioperasikan. Semua syarat pemilihan lokasi yang telah disebutkan dalam teori harus dipenuhi baik untuk bangunan kantor milik sendiri atau berlokasi di gedung perkantoran bersama.

Dalam kaitannya dengan daya listrik, gangguan yang mungkin terjadi adalah berupa gangguan ketidakstabilan listrik, interferensi gelombang radio dan elektromagnetik, dan listrik statis. Gangguan ketidakstabilan daya listrik dapat ditanggulangi secara murah dengan penggunaan UPS (*Uninterruptable Power Supply*) dan stabilizer.

Beberapa elemen yang cocok bagi UKM untuk memelihara keamanan fisik atas kontrol fasilitas sistem komputer adalah: penjaga, pagar, pencahayaan dan kunci. Semua kontrol diatas cocok untuk digunakan oleh UKM karena harganya yang tidak mahal, namun tidak perlu diterapkan semuanya tapi bergantung pada kebutuhaannya.

DAFTAR PUSTAKA

Krutz, R.L and Russel D. Vines, "*The CISSP® Prep Guide: Gold Edition"*, John Wiley Publising, Inc., 2003.

Wilson, Donald, "*eSecurity Guide for Small Business*", Association of Small Business DevelopmentCenter, http://download.microsoft.com/download/2/5/1/2518982c-228b-40a8-a7bf-f683b37a0f38/eSecurity GuideforSmallBusiness.pdf. Tanggal akses 29 November 2005.

Tipton, Harold. F, "*Information Security Management Handbook",* Auerbach Publishing Inc., 1999.