

SUPLEMEN MATERI KULIAH  
PROTEKSI & TEKNIK KEAMANAN SI/TI: IKI83408T

BAB 10  
PHYSICAL SECURITY

Disusun oleh:

Kelompok 124

**Ridwan Andi Kambau**  
**Riswan Efendi Tarigan**

**7203012203**  
**7204000616**



PROGRAM MAGISTER TEKNOLOGI INFORMASI  
UNIVERSITAS INDONESIA  
2005

# DAFTAR ISI

<b>DAFTAR ISI .....</b>	<b>(i)</b>
<b>DAFTAR GAMBAR .....</b>	<b>(iii)</b>
<b>DAFTAR TABEL .....</b>	<b>(iv)</b>
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1 Pengantar .....	1
1.2 Tujuan Penulisan .....	2
1.3 Profil Perusahaan .....	2
<b>BAB II <i>PHYSICAL SECURITY</i> .....</b>	<b>4</b>
2.1 <i>Physical Security</i> .....	4
2.2 Proses Perencanaan .....	8
2.3 <i>Facilities Management</i> .....	9
2.3.1 <i>Physical Attributes of the Facility</i> .....	10
2.3.2 Konstruksi .....	11
2.3.3 Komponen Fasilitas .....	13
2.3.4 Ruang Peralatan dan Komputer .....	15
2.4 Resiko Keamanan Fisik .....	16
2.5 Proses Pemilihan Komponen Keamanan Fisik .....	17
2.5.1 <i>Security Musts</i> .....	17
2.5.2 <i>Security Shoulds</i> .....	17
2.5.2.1 <i>Backups</i> .....	18
2.5.2.2 <i>Hardware</i> .....	18
2.5.2.3 <i>Power Supply</i> .....	19
2.6 Keadaan Lingkungan ( <i>Environmental Issues</i> ) .....	21
2.6.1 Ventilasi .....	23
2.6.2 Pencegahan, Deteksi, dan Pemadam Api .....	24
2.6.3 Tipe Pendeteksi Kebakaran .....	25
2.6.4 <i>Fire Detectors</i> .....	26
2.6.5 Pemadam Api .....	27

2.6.6 <i>Water Sprinklers</i> .....	28
2.7 <i>Pengawasan Administrasi (Administrative Controls)</i> .....	31
2.7.1 <i>Emergency Response and Reactions</i> .....	31
2.8 <i>Perimeter Security</i> .....	32
2.8.1 <i>Facility Access Control</i> .....	33
2.8.2 <i>Personnel Access Control</i> .....	36
2.8.3 <i>External Bondary Protection Mechanisms</i> .....	39
2.8.4 <i>Intrusion Detection Systems</i> .....	43
<b>BAB III KESIMPULAN</b> .....	<b>46</b>
<b>DAFTAR ACUAN</b> .....	<b>47</b>

## DAFTAR GAMBAR

Gambar 2.1	Diagram yang menunjukkan <i>power</i> , <i>air</i> , <i>sewer lines</i> , dan aliran dari data yang kritis yang perlu diperhatikan .....	9
Gambar 2.2	Contoh penyusupan lewat plafon .....	15
Gambar 2.3	Area yang diamankan harus memiliki hanya satu pintu masuk Dan harus diawasi .....	16
Gambar 2.4	Perangkat UPS mengkonversi arus DC dari batere menjadi AC dengan menggunakan inverter .....	20
Gambar 2.5	Pipa air, uap, dan gas harus memiliki katup <i>shutoff</i> keadaan darurat .....	22
Gambar 2.6	<i>Positive pressurization</i> yang menyebabkan asap keluar dari pintu	24
Gambar 2.7	Sistem <i>Dry Pipe</i> .....	29
Gambar 2.8	Jenis-Jenis Kunci .....	35
Gambar 2.9	Kartu berkomunikasi dengan proximity reader untuk memberikan akses .....	38
Gambar 2.10	Perangkat <i>perimeter scanning</i> bekerja melingkupi area tertentu	42

## DAFTAR TABEL

Tabel 2.1 Components Affected by Specific Temperatures .....	23
Tabel 2.2 Tiga Tipe Api dan Metode Pemadamannya .....	27
Tabel 2.3 <i>How Different Substances Interfere with Elements of Fire</i> .....	28

# **BAB I**

## **PENDAHULUAN**

### **1.1 Pengantar**

Sistem Keamanan merupakan salah satu bagian penting dalam setiap proses pengembangan suatu bisnis dan investasi, karena dengan sistem keamanan yang baik resiko atas kehilangan sejumlah nilai yang diinvestasikan menjadi lebih kecil. Dengan pesatnya perubahan teknologi dan usaha menerapkannya sebagai salah satu sarana berbisnis menyebabkan perubahan nilai informasi, sehingga mempengaruhi proses bisnis yang sedang berjalan. Melihat dari kondisi tersebut, membuat keamanan sistem informasi menjadi salah satu perhatian yang harus direncanakan dengan sebaik-baiknya. Oleh karena itu, keamanan sistem informasi harus terjamin dalam batas-batas yang dapat diterima.

Namun, keamanan informasi oleh banyak perusahaan masih dianggap sebagai masalah teknis yang cukup ditangani oleh salah satu bagian dari organisasi perusahaan, sehingga menghasilkan suatu solusi tanpa melihat dan menyesuaikan dengan proses bisnis yang ada. Artinya, perangkat sistem keamanan tercanggih pun sering kali belum mencukupi atau terlalu berlebihan untuk diterapkan. Sia-sia apabila kita menerapkan sistem TI dengan teknologi pengamanan mutakhir dan biaya sangat mahal kalau ternyata kebutuhan kita tidak serumit itu dan fungsinya pun tidak optimum, terutama bila bisnis yang kita lakukan hanya Usaha Kecil Menengah (UKM). Sebaliknya, tidak ada gunanya membeli sistem murah namun tidak dapat memberikan tingkat keamanan sistem yang diharapkan.

Pada kesempatan ini kelompok kami membahas tentang apa saja yang perlu diperhatikan untuk menerapkan suatu sistem keamanan khususnya keamanan secara fisik (*physical security*), yang disesuaikan dengan proses bisnis perusahaan skala kecil – menengah yang bergerak dalam jasa pelatihan teknologi informasi. Penerapan sistem keamanan yang digunakan disesuaikan dengan teori yang diberikan pada kelas proteksi dan sistem keamanan sistem informasi dan teknologi informasi.

## 1.2 Tujuan Penulisan

Suplemen ini bertujuan untuk membahas domain *physical security* dalam keamanan sistem informasi pada sebuah perusahaan skala kecil – menengah jasa pelatihan teknologi informasi yang berdomisili di Tangerang yaitu PT. Integrasi Lintas Buana.

## 1.3 Profil Perusahaan

PT. Integrasi Lintas Buana merupakan perusahaan jasa yang bergerak pada bidang pelatihan Teknologi Informasi. Didirikan pada awal tahun 2005 di pusat kota Tangerang. Dari awal berdirinya, perusahaan yang bergerak di bidang jasa ini, ingin memberikan layanan pelatihan TI bagi perusahaan pemerintah, swasta maupun perorangan yang ingin meningkatkan kemampuan dibidang Teknologi Informasi.

Pada mulanya, perusahaan berada disebuah ruko yang disewa pertahun, namun sejalan dengan perkembangannya, kini perusahaan memiliki gedung sendiri berlantai tiga.

Setiap hari, perusahaan beroperasi selama 12 jam dari Senin sampai Jumat dengan jadwal kelas (Reguler 09.00 – 16.00 WIB dan Intensif 17.00 – 21.00 WIB), serta beroperasi selama 5 jam di hari Sabtu dengan jadwal kelas Eksekutif 08.00 – 13.00 WIB). Perusahaan memiliki gedung 3 lantai berpusat di wilayah Tangerang.

Jumlah pegawai adalah 18 orang, terdiri dari 1 orang Direktur, 1 orang Sekretaris, 4 orang Marketing, 4 orang bagian Operasioal, 5 Orang Instruktur, 1 orang Bagian Keuangan, 1 orang *Driver*, dan 1 orang Office Boy.

Direktur bertanggung jawab terhadap semua kegiatan perusahaan untuk mencapai tujuan. Sekretaris Direktur bertanggung jawab untuk mengatur jadwal kegiatan direktur dan menerima surat masuk dan keluar dari *customer*. Bagian marketing bertanggung jawab untuk memprospek dan memasarkan produk jasa pelatihan baik kepada institusi pemerintahan, swasta, sekolah, maupun pribadi (retail). Bagian Operasioal bertanggung jawab untuk mempersiapkan semua kebutuhan kantor dan kebutuhan semua kelas yang sedang dan akan berjalan, baik dari sisi perlengkapan *hardware* dan *software*. Bagian pendidikan (instruktur) bertanggung jawab

mempersiapkan materi maupun modul pelatihan sesuai dengan kebutuhan *customer*. Bagian keuangan bertanggung jawab terhadap uang masuk (jasa pelatihan maupun jasa konsultan) dan uang keluar (pembayaran terhadap pihak luar). *Driver* bertanggung terhadap terhadap kendaraan operasional baik untuk kebutuhan direktur dan marketing. *Office Boy* untuk operasional kebersihan ruang lab dan meja kerja pegawai.

Untuk menunjang kegiatan usaha, perusahaan memiliki 5 ruang kelas. Tiga kelas terdiri dari 10 perangkat PC, 10 monitor LCD, 1 buah LCD projector, dan 1 buah hub (repeater). Dua kelas terdiri dari 5 perangkat PC, 5 monitor LCD, 1 buah TV 29", dan 1 buah hub (repeater). Perusahaan juga memiliki 5 buah router dan 5 buah switch Untuk menunjang lab Jaringan. Selain itu perusahaan juga memiliki perangkat kerja 2 unit Server (Proxy Server dan Mail Server), 16 PC beserta monitor untuk setiap pegawai yang menunjang pekerjaannya, 2 unit printer (1 printer untuk mencetak surat dan dokumen biasa, dan 1 printer warna untuk mencetak sertifikat serta dokumen tertentu).

Karena produk yang diperjualbelikan adalah jasa pelatihan Teknologi Informasi, serta semakin banyaknya bisnis serupa, maka dibutuhkan perencanaan sistem keamanan yang baik untuk menunjang dan menjaga aset perusahaan dalam kegiatan dan persaingan dengan kompetitor. Sistem keamanan yang diterapkan harus mempertimbangkan kemampuan dari pegawai dan lingkungan tempat perusahaan melakukan kegiatan, baik secara *software* maupun secara fisik.

## **BAB II**

### **PHYSICAL SECURITY**

Keamanan (*security*) adalah sangat penting bagi suatu perusahaan (baik skala kecil, menengah maupun *enterprise*) dan infrastruktur yang dimiliki, dan tidak terkecuali terhadap keamanan fisik (*physical security*). Keamanan fisik meliputi hal yang berbeda-beda yaitu ancaman (*threat*), keringkahan (*vulnerabilities*), dan resiko. Mekanisme keamanan fisik termasuk *site design* dan *layout*, komponen lingkungan (*environmental components*), kesiapan dalam merespon suatu kejadian (*emergency response readiness*), pelatihan, pengawasan akses (*access control*), deteksi penyusupan (*intrusion detection*), dan proteksi terhadap listrik dan kebakaran.

Praktisi *security* perlu waspada terhadap elemen yang mengancam *physical security* perusahaan dan pengontrolan dapat mengurangi resiko yang mendatangkan ancaman.

Domain *physical security* menunjukkan ancaman, kerawanan dan tindakan balasan yang dapat digunakan untuk proteksi fisik sumber daya perusahaan dan informasi rahasia. Sumber daya termasuk personel, fasilitas kerja, data, peralatan, sistem pendukung dan media kerja. *Physical security* kadang mengacu pada pengukuran yang diambil untuk melindungi orang, sistem, gedung dan infrastruktur lainnya terhadap ancaman yang berhubungan dengan lingkungan fisik.

Sementara keamanan fasilitas TI secara fisik adalah perlindungan terhadap aset teknologi informasi sebuah institusi yang ditempatkan di dalam area seperti gedung, *room*, *closet*, atau jalur bawah tanah. Saat perusahaan mendesain baru atau meng-*upgrade* fasilitas TI yang ada, merupakan prioritas tinggi untuk menempatkannya secara aman [1].

#### **2.1 Physical Security**

Keamanan fisik terhadap komputer dan sumber daya yang ada di tahun 1960-an dan 1970-an tidak serumit saat ini, karena komputer sebagian besar adalah *mainframe*

yang di kunci di ruangan *server* dan ditangani oleh orang-orang yang tahu bagaimana menanganinya.

Saat ini, hampir di setiap meja di setiap perusahaan ada komputer, perangkat, sumber daya yang disebar ke seluruh bagian, perusahaan yang lebih besar memiliki beberapa kabel yang dipasang di dinding dan ruang *server*, dan *remote*, dan *mobile user* yang menggunakan komputer dan sumber daya diluar fasilitas lokal. Dengan demikian perlindungan terhadap sistem komputer dan perangkatnya menjadi suatu yang pokok dan semestinya diperhatikan oleh sejumlah besar perusahaan, termasuk juga usaha kecil menengah (UKM).

Sebelum memulai investigasi berbagai cara yang dapat perusahaan lakukan untuk mengimplementasikan *physical security* yang tepat, maka perlu diketahui aspek apa saja dari lingkungan yang dapat menjadi ancaman bagi infrastruktur *computing* suatu perusahaan. Pada saat *Risk Analysis* dan *Business Impact Assesment* dilakukan, semua daftar ancaman yang mungkin harus disusun. Tidak jadi masalah jika kemungkinan kerawanannya rendah atau tidak ada (contohnya Tsunami di Aceh), semua kemungkinan ancaman harus disusun dan diperiksa. Banyak Metode penilaian (SSE-CMM atau IAM) memiliki pelaksana penyusunan daftar ancaman sebelum menetapkan pelaksanaannya. *Triad Confidentiality, Avalaibility, dan Integrity* adalah resiko dari lingkungan fisik dan harus dilindungi.

**Contoh Resiko CIA berikut ini :**

- Gangguan dalam menyediakan layanan komputer (A)
- Kerusakan Fisik (A)
- Penyingkapan Informasi bagi yang tidak berhak (C)
- Kehilangan Kontrol Sistem (I)
- Pencurian Barang (CIA)

**Contoh Ancaman Keamanan Fisik berikut ini:**

- Keadaan Darurat
  - Kontaminasi Api dan Asap
  - Gedung yang runtuh
  - Kehilangan Fasilitas (listrik, AC, pemanas)
  - Kerusakan (pipa) Air

- Pelepasan material beracun
- Bencana Alam
  - Pergerakan Bumi (Gempa Bumi, Longsor)
  - Badai ( Salju, es dan banjir)
- *Intervensi* Manusia
  - *Sabotase*
  - Perusakan
  - Perang
  - Pemogokan

Tujuh sumber kehilangan/kerusakan Fisik (Donn B.Parker)

1. Temperatur, variasi ekstrim panas dingin, seperti sinar matahari, api, pendinginan dan pemanasan.
2. Gas, perang gas, asap komersial, kelembaban, udara kering dan partikel dihentikan termasuk didalamnya. Contohnya Gas Saraf Sarin, PCP dari ledakan transformer, kegagalan AC, asap, kabut asap, cairan pembersih, kebocoran asap dan partikel kertas dari *printer*.
3. Cairan, Air dan termasuk cairan kimia. Contohnya banjir, kerusakan pipa, hujan salju, kebocoran bahan bakar, tumpahan air, asam dan zat kimia pembersih dan cairan *printer*.
4. Organisme, virus, bakteri dari orang, binatang, serangga termasuk didalamnya. Contohnya: jamur, kontaminasi dari kulit berminyak dan rambut, kontaminasi dan hubungan pendek dari pembuangan dan melepaskan cairan tubuh, konsumsi dari media informasi seperti kertas, isolasi kabel dan hubungan pendek rangkaian mikro dari jaringan.
5. Proyektil, Obyek nyata dalam pergerakan dan obyek bertenaga termasuk didalamnya. Contohnya meteor, obyek yang jatuh dari mobil dan truk, peluru dan roket, ledakan dan angin.
6. Pergerakan, Runtuh, cukur, kocok, getar, *lequefaction*, aliran, gelombang, pemisahan dan *slide* termasuk didalamnya. Contohnya menjatuhkan atau

menggerakkan perangkat mudah pecah, gempa bumi, pergerakan bumi, aliran lava, gelombang laut dan kegagalan perekat.

Anomali Energi, Tipe dari anomali listrik adalah gelombang listrik, magnetisasi, listrik statis, kontak lama, radiasi, suara, lampu, dan gelombang *microwave*, elektromagnet, gelombang atom. Contohnya kegagalan listrik, dekatnya magnet dan elektromagnet, karpet statis, dekomposisi dari *material circuit*, dekomposisi dari kertas dan *magnetic disk*, pulsa elektromagnet (EMP) dari ledakan nuklir, laser, *loudspeaker*, *HREF gun*, sistem radar, radiasi kosmis dan ledakan.

Pencurian dari orang dalam, penipuan, sabotase, dan kecelakaan telah meningkatkan biaya bagi sejumlah perusahaan karena lingkungan menjadi lebih kompleks dan dinamis. Banyak perusahaan berpengalaman kehilangan memori atau prosesor yang dicuri dari *workstation* dan sebagian mengambil komputer dan laptop. Perusahaan mungkin harus menggunakan *security guards*, *closed-circuit TV (CCTV)*, dan kamera terpasang, mengharuskan *user* menandai semua material, dan mengharuskan pegawai mereka untuk memiliki kepedulian yang lebih tinggi terhadap resiko-resiko tersebut. Pekerja kontrak atau paruh waktu boleh memiliki kartu akses khusus dan hanya diizinkan di area tertentu. Pengawasan akses yang lebih terbatas boleh diterapkan dengan kartu akses pribadi dan pendeteksi pergerakan, dan sistem infra merah juga boleh diinstal. Hanya ada beberapa item yang termasuk dalam batasan keamanan secara fisik, dan bila salah satunya tidak menyediakan tingkat perlindungan yang dibutuhkan, akan menyebabkan kelemahan yang dapat melanggar keamanan.

Keamanan secara fisik terbaik melalui fasilitas konstruksi, perlindungan kerusakan dari api dan air, mekanisme anti pencurian, sistem pendeteksi penyusupan (IDS), dan prosedur keamanan yang ada dan dilakukan. Komponen yang termasuk dalam tipe keamanan ini adalah fisik, teknikal, dan mekanisme pengawasan secara administratif.

Keamanan dibutuhkan untuk melindungi orang-orang dan perangkat keras. Keamanan harus meningkatkan produktivitas dengan menyediakan lingkungan yang aman dan dapat diprediksi. Hal ini memungkinkan tenaga kerja fokus terhadap

pekerjaan yang mereka tangani dan penjahat akan tahu untuk pindah ke bagian yang lebih ringkih dan target yang lebih mudah. Bagaimanapun, ini merupakan harapan.

Sebagian besar perhatian keamanan di *cyberspace*— *antivirus*, *firewalls*, *encryption* dan seterusnya tetapi bagaimana pengamanan asset Teknologi Informasi fisik, agar jangan sampai terjadi dimana seseorang berjalan ke luar pintu dengan membawa *server*, atau konsekuensi yang harus diterima karena lingkungan menjadi terlalu panas, kelembaban yang buruk atau suatu pipa air yang retak?

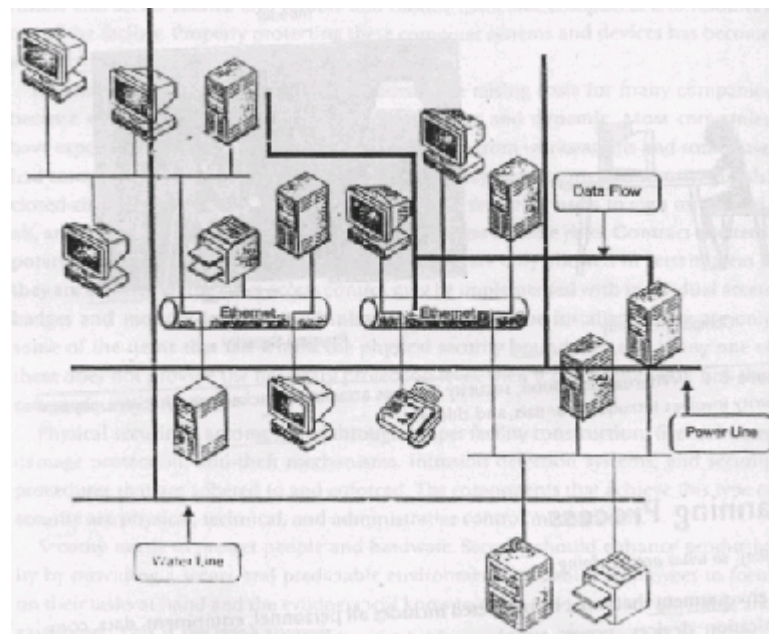
Keamanan fisik memiliki beberapa perbedaan keringkahan daripada keamanan informasi dan komputer. Keringkahan tersebut lebih pada pengrusakan secara fisik, penyusupan, masalah lingkungan, dan penyalahgunaan hak tenaga kerja dan mengakibatkan kerusakan yang tidak diharapkan terhadap data atau sistem. Bila seorang profesional di bidang keamanan memperhatikan keamanan komputer, mereka akan berfikir tentang bagaimana seseorang dapat masuk kelingkungan yang tidak dikehendaki melalui *port* atau *modem*. Bila mereka melihat keamanan secara fisik, mereka peduli dengan bagaimana seseorang secara fisik masuk ke lingkungan tertentu, bagaimana masalah lingkungan mempengaruhi sistem, atau tipe sistem pendeteksi penyusup apa yang terbaik untuk fasilitas tertentu. Setiap tipe keamanan memiliki masalah sendiri yang harus disadari dan di-*countermeasure* untuk diterapkan, tetapi lebih banyak seorang profesional keamanan tahu mengenai semua area keamanan, semakin menguntungkan karena dia mengerti bagaimana semua bagian saling berkaitan dan masing-masing saling tergantung.

## **2.2 Proses Perencanaan**

Lingkungan yang harus dilindungi termasuk semua orang, peralatan, data, perangkat komunikasi, *power supply*, dan kabel. Tingkat perlindungan yang diperlukan tergantung pada nilai data, sistem komputer, dan aset perusahaan di dalam fasilitas tersebut. Nilai dari setiap item dapat ditentukan dengan *critical-path analysis*, yang mendaftarkan setiap bagian dari infrastruktur dan apakah penting untuk menjaga bagian tersebut tetap sehat dan dapat beroperasi. Analisis ini juga menjelaskan jalur data yang diambil saat melintas melalui jaringan. Data dapat

melintas dari *remote user* ke *server*, dari *server* ke *workstation*, dari *workstation* ke *mainframes*, dan dari *mainframe* ke *mainframe* lainnya. Hal ini penting dimengerti mengenai jalur yang dilalui dan ancaman yang dapat mengganggunya.

*Critical-path analysis* mendaftarkan semua bagian dari lingkungan dan bagaimana mereka berinteraksi dan bagaimana saling ketergantungannya. Sebuah diagram harus dikembangkan untuk memperlihatkan semua perangkat dan tempatnya dan hubungannya terhadap fasilitas. Diagram tersebut harus mencakup *power*, *data*, *air*, dan jalur selokan. *Air conditioner*, *generator*, dan saluran udara juga termasuk untuk memberikan gambaran yang jelas dan mudah dimengerti. Gambar 2.1 menunjukkan contoh yang sederhana dari tipe diagram ini.



**Gambar 2.1** Diagram yang menunjukkan *power*, *air*, *sewer lines*, dan aliran dari data yang kritis yang perlu diperhatikan [3]

*Critical path* ditentukan sebagai jalur yang kritis untuk fungsi bisnis. *Critical path* harus ditampilkan secara rinci dengan semua mekanisme pendukung. *Redundant path* harus ditampilkan dan harus ada setidaknya satu *redundant path* untuk setiap *critical path*.

## **2.3 Facilities Management**

Fasilitas fisik biasanya berupa gedung sebagai tempat tinggal pegawai, peralatan, data dan perangkat jaringan. Manajemen fasilitas bertanggung jawab mulai dari sebelum gedung dibangun, dengan memilih lokasi, material, dan sistem pendukung yang tepat. Seringkali di perusahaan, manajer fasilitas direkrut secara penuh untuk bertanggung jawab terhadap semua sisi gedung dan masing-masing *interface* dengan *system administrator* dan staff manajemen untuk memastikan bahwa semua masalah yang tumpang tindih sudah disetujui sebelumnya dan dilindungi dengan semestinya.

### **2.3.1 Physical Attributes of the Facility**

Saat perusahaan memutuskan untuk membangun gedung, ada beberapa hal yang harus diperhatikan sebelumnya. Tentunya, harga tanah, populasi pelanggan, dan strategi pemasaran harus di-*review*, tetapi sebagai profesional keamanan, kita lebih tertarik terhadap keyakinan dan perlindungan lokasi tertentu yang dapat diberikan. Beberapa organisasi setuju terhadap kerahasiaan tertinggi atau keyakinan informasi membuat fasilitas mereka tidak dapat diperhatikan sehingga mereka tidak menarik perhatian pada penyerang. Gedung akan sulit dilihat dari pinggir jalan, tanda perusahaan dan logo kecil dan tidak mudah diperhatikan, dan penandaan gedung tidak memberi informasi apapun yang menyinggung ke dalam gedung. Ini adalah tipe kota atau *kamufalse* perkotaan yang membuatnya lebih sulit bagi musuh untuk mencarinya.

Beberapa gedung dibangun dimana dikelilingi oleh bukit atau pegunungan untuk membantu mencegah *eavedropping* sinyal listrik yang berasal dari perangkat fasilitas. Fasilitas lain dibangun dibawah tanah atau tepat di sisi gunung untuk menyembunyikan atau menyamarkan dilingkungan yang alami, dan melindungi dari peralatan radar dan kegiatan mata-mata. Hal ini biasanya untuk fasilitas yang sangat rahasia terutama yang dapat mengancam fasilitas suatu negara.

Pemilihan lokasi juga berarti mengidentifikasi tipe lain dari resiko yang berhubungan dengan area tertentu. Masalah tersebut berhubungan dengan

kemungkinan bencana alam, tingkat kejahatan, tetangga sekitarnya, dan kedekatan ke pelabuhan udara dan jalur kereta api. Jika perusahaan dibangun di area yang berpendapatan rendah, meskipun harga tanah kemungkinan lebih murah, hal ini akan membutuhkan tingkat keamanan fisik dan *perimeter* yang lebih tinggi, dimana akan mengakibatkan biaya yang melampaui batas.

Inspeksi terhadap fasilitas yang ada harus dilakukan untuk menampilkan kerentanan dan meluasnya kerentanan tersebut. Nilai *property* berikut fasilitasnya dan nilai fasilitas itu sendiri perlu dipastikan untuk menentukan anggaran semestinya yang harus disediakan terhadap keamanan fisik.

### **2.3.2 Konstruksi**

Materi konstruksi secara fisik dan komposisi struktur bangunan perlu dievaluasi terhadap karakteristik perlindungan, menilai utilitasnya, dan biayanya dan keuntungannya perlu dihitung. Perbedaan materi gedung memberikan tingkat perbedaan dari perlindungan terhadap api dan *combustibility*, yang berhubungan dengan *rating* api. Tipe materi konstruksi yang digunakan (kayu, beton, atau baja) perlu di kombinasikan dengan gedung yang dibangun saat membuat keputusan struktur. Bila area yang dibangun akan digunakan untuk menyimpan dokumen dan peralatan lama, akan jauh berbeda kebutuhannya dan memenuhi aturan hukum daripada jika area ini akan digunakan untuk pekerja yang bekerja setiap hari selama seminggu.

Ketika mendesain dan membangun fasilitas, bagian utama yang perlu diperhatikan sebagai titik pandang keamanan fisik, yaitu:

#### **Wails**

Materi yang mudah terbakar (kayu, baja, beton)

Rating api

Bala bantuan untuk area yang diamankan

#### **Pintu**

Materi yang mudah terbakar (kayu, *pressed board*, aluminium)

*Fire rating*

*Resistance to forcible entry*

*Emergency marking*

*Placement*

*Alarms*

*Directional opening*

Kunci pintu elektrik perlu diubah ke kondisi *disabled* bila terjadi kehilangan daya untuk proses evakuasi

*Type of glass* – bila perlu, harus tahan pecah atau tahan peluru

### **Langit-langit / plafon**

Materi yang mudah terbakar (kayu, baja, beton)

*Fire rating*

Tingkat kemampuan menahan beban

### **Jendela**

Kebutuhan tembus cahaya atau buram

Tahan pecah

Alarm

Penempatan

Kemudahan akses (penyusuk dapat merusaknya dan mengakses fasilitas)

### **Lantai**

Tingkat kemampuan menahan beban

Materi yang mudah terbakar (kayu, baja, beton)

*Fire rating*

*Raised flooring* (pentanahan listrik)

Materi dan permukaan yang tidak terkonduksi

### **Heating and Air Conditioning**

Tekanan udara positif

Lubang angin terlindung

*Dedicated power lines*

Switch dan katup *switch-off* dalam keadaan darurat

penempatan

### **Power Supplies**

Sumber daya utama dan cadangan

*Clean power source*

*Dedicated feeders to required areas*

Penempatan dan akses ke panel distribusi dan *circuit breakers*

### **Water and Gas Lines**

Katup shutoff

Aliran positif (materi harus mengalir keluar gedung, bukan masuk)

Penempatan

*Fire Detection and Suppression*

Penempatan sensor dan detector

Penempatan *sprinklers*

Tipe *detector* dan *sprinklers*

Profesional keamanan mungkin memerlukan fase perencanaan pembangunan fasilitas dan setiap bagian menjadi penting saat konstruksi gedung dan menghasilkan lingkungan yang aman.

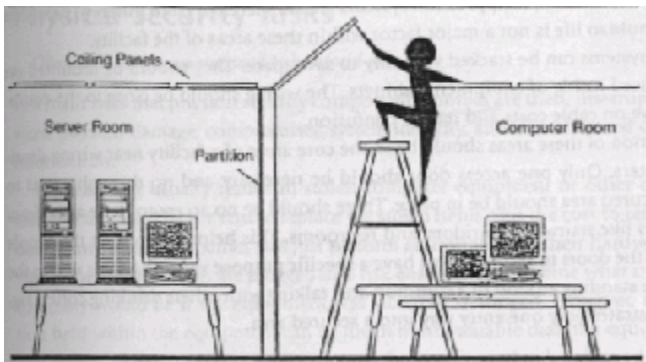
### **2.3.3 Komponen Fasilitas**

Ada banyak komponen yang menjadi fasilitas yang harus dilihat dari sudut pandang keamanan. *Internal partition* digunakan sebagai pemisah antara satu area dengan area lainnya. Partisi tersebut dapat juga digunakan sebagai pemisah jaringan, pemisah area kerja, dan memberikan perlindungan terhadap area sistem dan perangkat yang sensitif. Banyak gedung memiliki *hung ceiling*, yang berarti partisi bagian dalam tidak dapat di *extend* diatas langit-langit; oleh karena itu, seorang penyusup dapat naik ke panel langit-langit dan memanjat lewat partisi. Gambar 2.2 menunjukkan contoh penyusupan dari langit-langit.

Permukaan yang dapat menyalurkan listrik, bahkan listrik statis, harus dihindarkan dari tempat dimana perangkat listrik sensitif digunakan. Karpet dapat

diterima di area kerja pegawai, tetapi tidak digunakan di ruangan *server* atau tempat pemasangan kabel.

*Data center* biasanya peralatan yang mahal dan dimiliki perusahaan yang memiliki data yang kritis; oleh karenanya, perlindungan harus disiapkan sebelum implementasi. *Data center* harus ditempatkan diatas lantai gedung untuk menghindari api dan diluar *basement* untuk menghindari banjir. *Data center* biasanya harus ditempatkan dibagian utama dari gedung untuk memberikan perlindungan dari bencana alam atau bom dan memberikan kemudahan akses bagi 'anggota keadaan darurat' bila dibutuhkan. Harus ditempatkan di area yang sedikit tertutup/terpencil untuk membatasi akses dan tidak disamping kafetaria atau area lain dimana pegawai berkumpul.



**Gambar 2.2** Contoh penyusupan lewat plafon [3]

Sesuatu dari lingkungan eksternal juga perlu diperhatikan. Perusahaan harus mengevaluasi seberapa dekat fasilitas yang ada ke kantor

polisi, pemadam kebakaran, dan fasilitas rumah sakit. Seringkali, kedekatan tersebut menaikkan nilai *real estate* dari properti tersebut, tetapi untuk alasan yang baik. Bila perusahaan kimia yang memproduksi materi yang berdaya ledak tinggi butuh membangun fasilitas yang baru, hal ini membuat bisnis lebih baik dengan menemukannya dekat dan mudah diakses ke pemadam kebakaran terdekat. Bila perusahaan lain yang dibangun dan menjual perangkat elektronik yang mahal berkembang dan perlu berpindah operasi ke fasilitas lain, waktu reaksi polisi boleh dilihat saat memilih satu area dari area lainnya. Masing-masing hal tersebut, kantor polisi, pemadam kebakaran, dan fasilitas kesehatan terdekat, dapat juga mengurangi tingkat jaminan/asuransi, dan harus diperhatikan secara hati-hati.

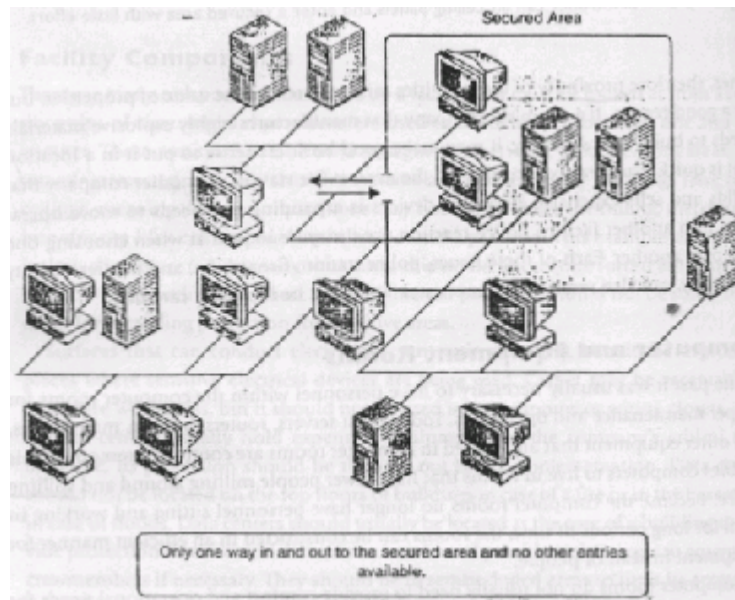
### 2.3.4 Ruang Peralatan dan Komputer

Di masa lalu biasanya diperlukan orang di dalam ruangan komputer untuk mengoperasikan dan memeliharanya. Sekarang kebanyakan *server*, *router*, *bridge*, *mainframe*, dan peralatan lain ditempatkan tersendiri di ruang komputer dan di awasi dari jarak jauh. Hal ini memungkinkan komputer aktif di ruangan yang hanya memerlukan sedikit orang yang berdesakan dan dapat menumpahkan kopi. Karena ruang komputer tidak lagi memerlukan orang yang duduk dan bekerja ditempat tersebut untuk waktu yang lama, ruangan dapat dikonstruksi secara efisien yang khusus untuk peralatan tanpa orang.

Ruang komputer biasanya tidak butuh menyediakan operasi yang nyaman layaknya yang dibutuhkan orang; dengan demikian ruangan komputer dapat dibuat kecil dan sistem pemadam api yang mahal tidak dibutuhkan lagi. Di waktu lampau pemadam api Halon adalah cara yang paling terkenal untuk melindungi pegawai yang bekerja di ruangan komputer. Sistem tersebut sangat mahal untuk diinstal dan dielihara. Sistem pemadam api memang masih diperlukan, tetapi dengan tipe yang berbeda yang dapat digunakan bila hidup manusia bukan menjadi faktor utama didalam area fasilitas tersebut.

Sistem yang lebih kecil dapat di tempatkan secara vertikal untuk menghemat ruangan. Mereka harus di pasang di rak atau ditempatkan didalam peralatan *cabinet*. Kabel harus dekat dengan peralatan untuk menghemat biaya kabel dan tidak membingungkan.

Lokasi area tersebut harus di area utama dari fasilitas yang dekat dengan pusat pembagian kabel. Hanya satu pintu masuk yang diperlukan dan tidak ada akses langsung ke ruangan yang tidak aman. Harus tidak ada akses ke area tersebut dari area umum seperti tangga, koridor, dan toilet. Hal ini membantu untuk memastikan bahwa orang yang masuk lewat pintu ke area yang diamankan memiliki tujuan khusus dibanding mereka berjalan ke toilet atau berdiri disekitar area umum saling berbicara dan sambil minum kopi. Gambar 2.3 mengilustrasikan hanya ada satu jalan masuk ke area yang diamankan.



**Gambar 2.3** Area yang diamankan harus memiliki hanya satu pintu masuk dan harus diawasi [3]

## 2.4 Resiko Keamanan Fisik

Resiko utama yang ingin diberantas dari komponen keamanan fisik adalah, pencurian, gangguan layanan, kerusakan fisik, integrasi sistem yang *compromised*, dan penyingkapan informasi yang tidak diizinkan.

Pencurian fisik biasanya peralatan komputer atau perangkat lainnya. Kerugian sebenarnya ditentukan oleh biaya pengganti dari barang yang dicuri ditambah biaya pemulihan data yang hilang. Seringkali perusahaan hanya akan melakukan inventaris dari perangkat keras dan menyediakan nilai perkiraan dengan memasukkan ke analisis resiko untuk menentukan biaya apa saja bagi perusahaan bila seandainya peralatan dicuri atau rusak. Bagaimanapun, informasi yang ada didalam peralatan tersebut dapat lebih bernilai daripada peralatan itu sendiri, dan mekanisme pemulihan yang baik dan prosedur juga perlu dimasukkan ke dalam penilaian resiko agar lebih realistis dan seimbang.

Gangguan *services* dapat menghilangkan layanan komputer, sumber daya, suplai air, dan layanan telekomunikasi.

## **2.5 Proses Pemilihan Komponen Keamanan Fisik**

Semua mekanisme perlindungan harus memberikan keuntungan dari biaya bagi perusahaan dan komponen keamanan fisik pun demikian. Mekanisme keamanan yang merupakan keuntungan dari biaya maksudnya bahwa mengurangi kehilangan potensial secara signifikan akan lebih baik daripada biaya implementasi mekanisme di tempat utama dan perawatan selanjutnya. Realisasi ini perlu dikumpulkan fakta yang rinci dan tepat, penilaian dan analisis resiko, dan *review* dari semua mekanisme yang tersedia yang dapat memberikan tipe perlindungan yang sama.

Untuk memilih komponen keamanan fisik, ada beberapa "*musts*", beberapa yang "*shoulds*" yang harus dipahami dengan jelas sehingga keputusan yang baik dapat dilakukan.

### **2.5.1 Security Musts**

Sebagian besar perusahaan terikat oleh hukum untuk mematuhi kebutuhan keamanan tertentu. Sebuah gedung, harus memiliki tangga disamping *elevator*, harus memiliki *fire alarm* dan detektor asap, harus memiliki tanda *exit* dan mudah dilihat, dan pintu keluar api tidak boleh diblok dan harus memiliki lokasi *panic bars* sebagai tempat evakuasi orang-orang bila terjadi keadaan darurat. Hal ini harus diimplementasikan dan diperlukan secara hukum, tidak masalah seberapa mahal biaya bagi perusahaan.

### **2.5.2 Security Shoulds**

Ada prosedur perlindungan yang harus ditempatkan untuk membantu melindungi perusahaan dari aktivitas yang merusak dan hasil yang didapatkan. Sering kali prosedur perlindungan menggunakan komponen keamanan yang sudah ada di sekitar lingkungan, karena itu, tidak memerlukan anggaran tambahan. Prosedur tersebut termasuk: *backing up* data yang kritis, konfigurasi komponen keamanan yang merupakan bagian dari sistem operasi dan perangkat keras disamping juga membeli peralatan yang menyediakan fungsi yang sama, memperhatikan aktivitas

pegawai yang mencurigakan, membagi jaringan secara logika dan fisik, dan mempunyai *safety guard* yang berjalan disekitar departemen, tidak hanya ditempatkan di satu area.

Bila ada mekanisme perlindungan keamanan yang berbiaya rendah tetapi memberikan keuntungan secara material, maka mekanisme tersebut harus di implementasikan. Kunci adalah peralatan pencegahan yang tidak terlalu mahal, tetapi dapat melindungi fasilitas dan isinya dari pencurian dan pengrusakan. Jadi untuk semua mekanisme keamanan yang berbiaya rendah, tetapi dengan keuntungan signifikan, harus diimplementasikan.

### **2.5.2.1 Backups**

Tidak setiap data harus di-*backup*, oleh sebab itu penting mengenali mana data yang kritis, penting, dan biasa. Ini adalah proses prioritas untuk memilah jenis-jenis data, aplikasi, dan kode program. Adalah penting menentukan prioritas mana yang harus di *backup* bila terjadi keadaan darurat dan segera dapat dipulihkan kembali. Program yang memungkinkan fasilitas yang berbeda untuk komunikasi dan akses data ke sistem *host*, dan aplikasi yang melindunginya dan proses informasi yang kritis terhadap bisnis harus dapat diakses secara *online* dan jaminan dapat berfungsi dengan baik. Prioritas utilisasi akan memberikan jadwal yang realistis, memastikan pekerjaan yang kritis dapat dilakukan tepat pada waktunya, dengan biaya yang layak.

Lebih dari sekedar data yang harus di *backup* pada tempat dan waktu dia dibutuhkan. Perangkat keras, suplai daya listrik, dan sumber daya manusia, semua adalah bagian yang penting agar lingkungan proses data dapat berjalan dengan baik dan lancar.

### **2.5.2.2 Hardware**

Banyak perusahaan mengimplementasi tempat alternatif untuk membantu proses *recovery* setelah terjadi bencana. Dalam kondisi tidak terjadi bencana di kedua tempat tersebut; dengan begitu, ukurannya harus jelas. Semakin jauh antara kedua

tempat, semakin baik faktor keamanannya, tetapi meningkatkan biaya transportasi bagi pegawai, peralatan, dan data. Jika tempat sekunder harus digunakan maka harus ditentukan biaya untuk mencapai tempat tersebut serta menempatkan orang yang tepat. Tetapi, jika operasinya perlu dilakukan di tempat sekunder selama sebulan dan jaraknya di atas 100 mil, biaya hidup dan ongkos perjalanan bagi pegawai adalah biaya yang perlu dipertimbangkan. Selain terjadinya bencana utama, menyediakan *redundancy hardware* juga penting untuk keadaan darurat yang lebih kecil. Bila *file server* tertentu menyediakan layanan yang diperlukan secara kritis kepada perusahaan selama 24 jam sehari, 7 hari seminggu, biasanya digunakan kapabilitas RAID untuk melindungi data.

Namun untuk perangkat kerasnya sendiri, biasanya ada Service Level Agreements (SLA) antara perusahaan dan pemasok, sebagai jaminan *service level* yang perlu untuk perlindungan.

### **2.5.2.3 Power Supply**

Karena komputasi sudah menjadi bagian yang begitu penting bagi dunia bisnis, saat ini kegagalan daya listrik merupakan kejadian yang paling banyak merusak daripada 10 sampai 15 tahun yang lalu.

Dengan begitu, perlu perencanaan yang baik agar aset perusahaan tidak mengalami kehancuran akibat badai, angin tinggi, kegagalan perangkat keras, kilat atau sebab lain yang bisa menghentikan atau mengganggu persediaan daya listrik.

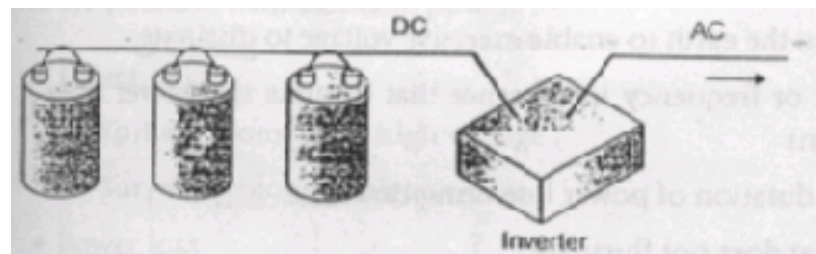
Ada beberapa tipe *backup* daya dan memilih yang terbaik sebaiknya dilakukan setelah dihitung biaya total bila terjadi *downtime* dan efek yang terjadi. Informasi ini bisa didapatkan dari catatan yang lalu serta dari perusahaan lain di bidang yang sama. Membagi belanja tahunan, dengan menghitung waktu standar tahunan dari penggunaan biaya total perjam dari *backup power*.

Ada beberapa persoalan besar dan kecil yang diakibatkan oleh kerusakan listrik atau fluktuasi. Efeknya menimbulkan variasi frekuensi, amplitudo, dan voltase dalam hitungan milidetik sehari. Perusahaan bisa mempunyai dua penyedia daya yang berbeda untuk mengurangi risiko, tetapi melakukan ini bisa teramat mahal.

Mekanisme yang lebih baik dan tidak terlalu mahal dengan memiliki pembangkit tenaga listrik (generator) sendiri. Beberapa generator mempunyai *sensors* untuk mengetahui kerusakan listrik utama dan akan mengambil alih secara otomatis.

Batas ambangnya bisa disesuaikan untuk memberikan layanan terbaik, tergantung pada tipe dan ukuran generator, untuk menyediakan daya selama sekian menit atau sehari penuh.

Ada tiga metode utama untuk perlindungan masalah daya: *uninterrupted power supply* (UPS), *power line conditioners*, dan *backup sources*. UPS menggunakan aki dalam ukuran dan kapasitas tertentu. UPS bisa *online* atau *standby*. Sistem *online* menggunakan tegangan AC untuk mengisi aki. Saat digunakan, UPS mempunyai *inverter* yang merubah keluaran DC dari aki ke bentuk AC yang dibutuhkan dan menyediakan tegangan sebagai sumber daya bagi perangkat komputer. Proses konversinya ditunjukkan oleh Gambar 2.4



**Gambar 2.4** Perangkat UPS mengkonversi arus DC dari batere menjadi AC dengan menggunakan *inverter* [3]

Sementara *Standby* UPS dalam keadaan tidak aktif sampai jalur listrik gagal. Sistem mempunyai *sensors* yang mengetahui kegagalan listrik dan beban dialihkan ke aki.

*Backup power supplies* diperlukan kalau ada kegagalan listrik yang lebih lama daripada yang dapat ditanggulangi oleh UPS. Suplai *backup* di dapat dari sumber listrik lainnya atau dari generator motor dan dapat digunakan untuk menyuplai daya utama atau mengisi aki sistem UPS.

Sistem yang kritis memerlukan perlindungan dari sumber daya yang terputus perlu dikenali dan diperkirakan seberapa lama daya sekunder diperlukan dan berapa banyak tenaga diperlukan untuk masing-masing perangkat. Beberapa UPS hanya

memberikan cukup daya saja untuk melakukan sistem *shutdown* secara baik, ada juga yang mampu menyuplai daya bagi sistem dalam jangka waktu yang lebih panjang. Perlu juga ditentukan jika sistem mempunyai cukup sumber listrik untuk melakukan *shutdown* dan *running* kembali untuk menyediakan layanan yang kritis.

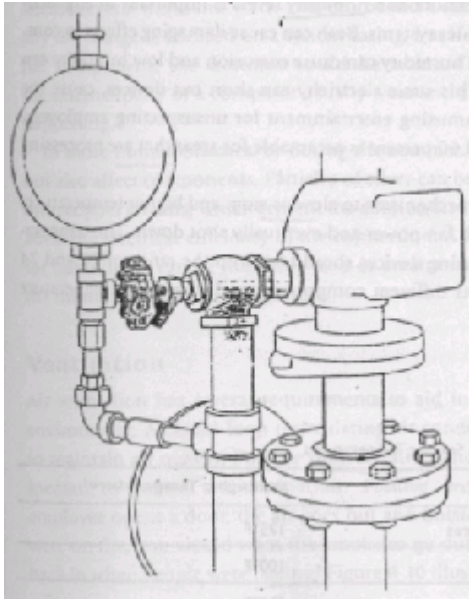
Mempunyai pembangkit tenaga listrik (generator) hanya akan memberi perasaan nyaman yang kabur bagi perusahaan. Sumber daya alternatif sebaiknya diuji secara berkala untuk memastikan perangkat tersebut dapat bekerja sesuai dengan yang diharapkan ketika terjadi suatu keadaan darurat. Tidak baik bila kemudian diketahui bahwa pembangkit tenaga listrik tidak bekerja dengan benar ketika keadaan darurat terjadi.

Untuk perusahaan berskala UKM, terkadang dibutuhkan generator seperti ini untuk mengambil alih suplai sumber daya listrik bila suplai daya dari PLN terganggu untuk jangka waktu yang tidak terlalu lama.

## **2.6 Keadaan Lingkungan (Environmental Issues)**

Pengawasan lingkungan yang tidak benar atau utilitas lingkungan yang tak diawasi bisa menyebabkan kerusakan layanan, perangkat keras, dan hidup itu sendiri. Layanan sistem dapat terganggu yang mengakibatkan hasil yang tidak diramalkan atau diperkirakan sebelumnya. Daya listrik, *heating*, ventilasi, pengaturan suhu udara (AC), dan kontrol mutu udara akan menjadi kompleks dan terdiri dari banyak variabel. Semuanya perlu dioperasikan dengan semestinya dan diamati secara teratur.

Selama pembuatan fasilitas, harus dipastikan bahwa katup air, uap, dan jalur gas dalam keadaan *shutoff*, dan *positive drains*, yang berarti isinya akan mengalir keluar area. *Positive drains* ditunjukkan pada Gambar 2.5. Bila ada gangguan di pipa air utama, aliran air harus dapat dimatikan. Kalaupun terjadi banjir disekitarnya, perusahaan ingin memastikan bahwa tidak ada fasilitas yang terendam air. Bila ada api didalam gedung, jalur gas harus dapat dihentikan. Bagian fasilitas, operasi, dan keamanan sebaiknya tahu di mana katup tersebut dan sebaiknya ada prosedur yang jelas untuk diikuti bila terjadi keadaan darurat. Hal ini akan membantu mengurangi kerusakan yang mungkin terjadi secara keseluruhan akibat bencana yang terjadi.



**Gambar 2.5** Pipa air, uap, dan gas harus memiliki katup *shutoff* keadaan darurat.[3]

Kebanyakan perlengkapan elektronik harus beroperasi dalam suasana iklim yang terkontrol. Walaupun penting untuk menjaga suasana kerja dalam suhu yang baik, perlu juga dimengerti bahwa ada komponen di dalam perlengkapan akan bermasalah bila mendapat panas berlebihan. Sering kali kipas internal komputer dalam keadaan kotor atau mampet, sehingga bagian dalam komputer mengalami panas secara berlebihan. Bila perangkat terlalu panas, ada bagian yang dapat memuai, yang berakibat sifat elektroniknya berubah, mengurangi keefektifan atau bahkan merusak kerja sistem secara keseluruhan.

Memelihara tingkat suhu dan kelembaban yang baik, penting di bagian fasilitas yang mana pun, terutama fasilitas sistem komputer. Karena bila kedua hal tersebut tidak diperhatikan, bisa menyebabkan kerusakan pada komputer dan alat listrik. Kelembaban tinggi bisa menyebabkan korosi dan kelembaban rendah bisa menyebabkan listrik statis berlebihan. Kelembaban relatif antara 45 sampai 60 persen dapat diterima untuk area yang berfungsi mengolah data.

Suhu lebih rendah bisa membuat mekanisme menjadi lambat atau berhenti, dan suhu yang lebih tinggi bisa membuat alat menggunakan terlalu banyak daya kipas/fan dan akhirnya *shutdown*. Suhu di area yang berisi peralatan komputer sebaiknya pada tingkat 70 dan 74 derajat Fahrenheit. Tabel 2.1 daftar komponen yang berbeda dan tingkat suhu merugikan.

**Tabel 2.1** Components Affected by Specific Temperatures [3]

<b>Material or Component</b>	<b>Damaging Temperature</b>
Computer systems and peripheral devices	175°F
Magnetic storage devices	100°F
Paper products	350°F

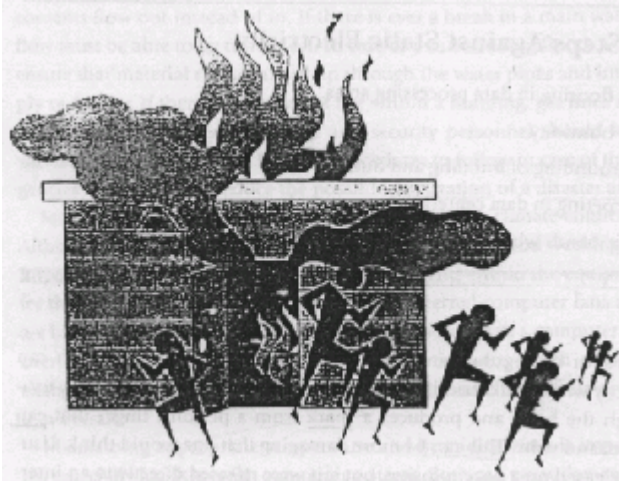
Di iklim yang lebih kering, atau selama musim dingin, udara hanya berisi sedikit embun, yang bisa mengakibatkan listrik statis bila dua objek berbeda saling bersentuhan. Listrik ini biasanya mengalir lewat badan dari peralatan dan mengeluarkan kilatan yang bisa melepaskan beberapa ribu volt. Ini bisa mengakibatkan kerusakan lebih dari yang terpikirkan. Biasanya arus listrik dilepaskan di atas sistem *casing*, tetapi bila dilepaskan langsung ke komponen dalam, akibatnya bisa lebih buruk. Oleh karena itu mengapa orang yang bekerja di bagian internal komputer biasanya memakai lengan *anti-static* untuk mengurangi kontak langsung.

Di iklim yang lebih lembab, atau selama musim panas, kelembaban tinggi di udara juga bisa mempengaruhi komponen. Partikel bisa berpindah dari konektor ke kontak tembaga, dimana semen konektor ke dalam stopkontak. Hal ini bisa mempengaruhi efisiensi hubungan listrik. *Hygrometer* biasanya digunakan untuk memantau kelembaban. Informasi dapat dibaca secara manual atau dipasang *alarm-off* otomatis jika kelembaban mencapai batas ambang tertentu.

### **2.6.1 Ventilasi**

Ventilasi udara mempunyai beberapa syarat untuk membantu memberikan lingkungan aman dan nyaman. Sistem pengaturan suhu sirkulasi tertutup harus dipasang untuk memelihara kualitas udara. Tekanan udara positif dan ventilasi juga sebaiknya diimplementasi untuk mengawasi pencemaran/kontaminasi. Tekanan udara positif/*positive pressurization* artinya bahwa kalau seorang pegawai membuka pintu,

udara akan keluar dan udara luar tidak masuk. Ilustrasi *positive pressurization* selama terjadi kebakaran ditunjukkan Gambar 6.



**Gambar 2.6** *Positive pressurization* yang menyebabkan asap keluar dari pintu [3]

Kontaminan perlu dimengerti bagaimana mereka memasuki lingkungan, kerusakan yang terjadi, dan langkah untuk menjamin bahwa fasilitas terlindung dari bahan berbahaya

atau kadar tinggi dari rata-rata kontaminan. Bahan yang dapat mengudara dan konsentrasi partikel harus diamati bila mencapai tingkat yang tak seharusnya. Debu bisa menyumbat fan/kipas yang berfungsi untuk menyejukkan suhu peralatan. Konsentrasi gas yang berlebihan bisa mempercepat korosi dan menyebabkan masalah *performance* atau kegagalan perangkat elektronik. Walaupun kebanyakan *disk drives* ditutup rapat, alat penyimpanan lain bisa dipengaruhi oleh kontaminan yang mengudara. Perangkat kualitas udara dan sistem ventilasi cocok untuk persoalan ini.

### 2.6.2 Pencegahan, Deteksi, dan Pemadam api

Masalah keamanan fisik tidak akan lengkap bila tidak membahas mengenai *fire safety*. Ada standar lokal dan standar nasional yang harus dipenuhi untuk metode pencegahan, deteksi, dan pemadam api. Pencegahan kebakaran dimulai dengan pemberian latihan kepada pegawai bagaimana caranya untuk bereaksi dengan semestinya kalau menghadapi api, menyediakan perlengkapan yang benar dan jaminan bahwa perlengkapan itu bekerja dengan baik, meyakinkan ada persediaan air yang mudah dicapai, dan menyimpan elemen yang mudah terbakar di tempat tertentu. Sistem respon pendeteksi api terdiri dari bentuk yang berbeda. Ada *the red manual pull boxes* yang dapat kita lihat di banyak tembok gedung perusahaan. Ada detektor yang otomatis, mempunyai *sensors* yang bereaksi kalau mereka mengetahui adanya

api. Sistem otomatis bisa berupa sistem alat penyembur (*sprinkler system*) atau *Halon discharge system*. *Automatic sprinkler system* secara luas dipakai dan sangat efektif untuk melindungi gedung dan isinya. Ketika memutuskan tipe sistem pemadam api mana yang akan dipasang, banyak faktor yang perlu dievaluasi termasuk perkiraan tingkat kemungkinan terjadinya kebakaran, banyaknya kerusakan yang diakibatkan, dan tipe sistem mana yang akan dipilih.

Perlindungan api terdiri atas deteksi asap awal dan *shutdown* sistem sampai sumber panas dapat dihilangkan sehingga kebakaran tidak terjadi. Jika perlu, sistem otomatis sebaiknya men-*shutdown* semua sistem. Tanda peringatan terlebih dulu berbunyi dan menahan tombol yang ada untuk menunda proses *shutdown* bila masalah dapat diatasi dan bahaya sudah terlewati.

### **2.6.3 Tipe Pendeteksi Kebakaran**

Kebakaran api menimbulkan ancaman keamanan yang sangat berbahaya karena api bisa merusak perangkat keras, data, dan resiko hidup manusia. Asap, suhu tinggi, dan gas korosif dari api bisa menyebabkan kehancuran; dengan begitu, penting mengevaluasi ukuran keamanan api terhadap gedung dan bagian-bagiannya.

Kebakaran api dimulai karena sesuatu sebagai sumbernya. Sumber nyala bisa terjadi karena kegagalan alat listrik, penyimpanan tidak patut dari bahan yang mudah terbakar, membuang rokok sembarangan, panas yang tinggi dari perangkat yang gagal fungsi, dan pembakaran yang disengaja. Api memerlukan bahan bakar dan oksigen untuk terus membakar dan bertambah besar; lebih banyak bahan bakar per meter persegi, lebih hebat api akan menjadi. Fasilitas sebaiknya dibuat, dipelihara, dan dijalankan dengan sesedikit mungkin penumpukan bahan bakar yang bisa mengakibatkan kebakaran.

Ada tiga kelas (A, B, dan C) api yang mungkin terjadi. Penting diketahui perbedaan di antara tipe api sehingga kita tahu bagaimana caranya untuk membedakannya. Alat pemadam api mempunyai tanda yang menunjukkan alat tersebut dipakai untuk tipe api tertentu. Tanda menunjukkan jenis bahan kimia didalam teromol dan tipe api yang dapat dipadamkan. Alat pemadam yang mudah

dibawa biasanya diisi dengan karbon dioksida (CO<sub>2</sub>) atau asam soda dan sebaiknya ditempatkan dalam radius 50 kaki dari perlengkapan listrik yang mana pun dan dapat ditemukan dekat jalan keluar. Alat pemadam sebaiknya ditandai secara jelas, dengan pandangan yang tak terhalang. Mereka sebaiknya dengan mudah dapat dicapai dan mudah dioperasikan oleh pegawai, dan diperiksa setiap bulan.

Banyak sistem terbuat dari bahan yang tidak mudah pembakaran, tetapi akan mencair atau hangus jika terlalu panas. Kebanyakan rangkaian komputer hanya mengkonsumsi dua sampai lima volt AC, yang biasanya tidak bisa menyebabkan terjadinya api. Sekering ditambahkan, agar alat tersebut *shutdown* jika mengalami panas yang tinggi.

#### **2.6.4 Fire Detectors**

Ada beberapa tipe detektor api, masing-masing bekerja dengan cara berbeda dan dengan tujuan berbeda pula. Semuanya memiliki termal yang dapat merasakan bila terjadi kebakaran dan merespon perubahan temperatur yang naik secara berkelanjutan. Detektor bisa diaktifkan dengan panas, asap, nyala api, atau partikel pembakaran.

**Smoke Activated** Detektor yang diaktifkan dengan asap adalah detektor yang baik bagi perangkat untuk peringatan awal. Mereka dapat dipergunakan untuk membunyikan alarm sebelum alat penyemur air berputar. *Photoelectric device*, juga dirujuk sebagai detektor optik, mengetahui perubahan arus listrik bila ada variasi pada intensitas cahaya. Detektor menghasilkan bias cahaya melintasi daerah yang dilindungi dan jika balok terhalang, alarm mengasumsikan ada asap dan kemudian berbunyi.

**Head Activated** Detektor yang diaktifkan panas dapat berupa alarm saat temperatur mencapai tingkat yang menguatirkan atau mendeteksi pertambahan temperatur yang melebihi tingkat tertentu, atau kombinasi dari keduanya. *Rate-of-rise temperature sensors*, biasanya memberikan peringatan yang lebih cepat daripada *fixed-temperature sensors* karena mereka lebih peka, tetapi dapat juga menyebabkan

alarm yang palsu. Sensor dapat diberi jarak secara seragam sepanjang fasilitas atau jalur instalasi, yang dioperasikan dengan kabel yang peka terhadap panas.

**Flame Activated** Alat yang diaktifkan dengan nyala api akan merasakan debaran nyala api atau merasakan energi inframerah yang dihubungkan dengan nyala api dan pembakaran. Alat yang diaktifkan dengan nyala api lebih mahal daripada tipe detektor api yang lain dan biasanya hanya digunakan untuk kasus tertentu ketika peralatan yang bernilai tinggi perlu dilindungi. Alat ini bisa merespon lebih cepat daripada detektor lain, melepaskan agen pemadaman, dan membunyikan alarm.

**Automatic Dial-up Alarm** Tipe sistem ini dikonfigurasi untuk memanggil pos pemadam kebakaran lokal, dan mungkin juga kantor polisi, untuk melaporkan terjadinya kebakaran. Seringkali sistem ini digabungkan dengan salah satu sistem pendeteksi yang disebutkan sebelumnya dan menambahkan fungsi lainnya.

### 2.6.5 Pemadam Api

Perlu diketahui tipe kebakaran api yang bisa terjadi dan apa yang sebaiknya dilakukan untuk memadamkannya. Setiap tipe api mempunyai tingkat yang mengindikasikan materi apa sebenarnya yang menyebabkan api.

Tabel 2.2 menampilkan tiga tipe api dan metode pemadamannya yang sebaiknya diketahui oleh semua pegawai.

**Tabel 2.2** Tiga Tipe Api dan Metode Pemadamannya [3]

<b>Fire Class</b>	<b>Type of Fire</b>	<b>Elements of Fire</b>	<b>Suppression Method</b>
A	Common combustibles	Wood products, paper, and laminates	Water or soda acid.
B	Liquid	Petroleum products and coolants	Gas (Halon), CO <sub>2</sub> , or soda acid
C	Electrical	Electrical equipment and wires	Gas (Halon), CO <sub>2</sub>

Ada beberapa cara untuk memadamkan kebakaran api, dan tindakan pencegahan tertentu yang sebaiknya diambil. Di banyak gedung, ada agen pemadam yang ditempatkan di area yang berbeda yang didesain untuk memulai memicu alat tertentu yang sudah terpasang. Masing-masing agen mempunyai zona liputan, area yang dibawah tanggung jawab agen. Jika kebakaran terjadi di zona tertentu, agen bertanggung jawab untuk memadamkannya. Ada tipe yang berbeda dari agen pemadaman: sebagian menggunakan air, Halon, atau CO<sub>2</sub>. Jika agen menggunakan CO<sub>2</sub>, sebaiknya mempunyai mekanisme penundaan didalamnya. Mekanisme penundaan/pelambatan untuk meyakinkan bahwa agen tidak mulai menggunakan CO<sub>2</sub> ke area tersebut sampai setelah alarm berbunyi dan orang-orang sudah diberi waktu untuk mengungsi. CO<sub>2</sub> adalah bahan tanpa bau dan tanpa warna yang mungkin bersifat mematikan, karena menyingkirkan oksigen dari udara. Masker gas tidak menyediakan perlindungan untuk melawan CO<sub>2</sub>; dengan demikian, tipe mekanisme pemadaman api jenis ini lebih baik dipakai di fasilitas dan area yang tidak ada orang. Api memerlukan bahan bakar, oksigen, dan temperatur yang tinggi. Tabel 2.3 menampilkan bahan pemadam yang mengatasi elemen api ini.

**Tabel 2.3** *How Different Substances Interfere with Elements of Fire* [3]

<b>Combustion Elements</b>	<b>Suppression Methods</b>	<b>How Suppression Works</b>
Fuel	CO <sub>2</sub> and soda acid	Removes fuel and oxygen
Oxygen	CO <sub>2</sub> and soda acid	Removes fuel and oxygen
Temperature	Water	Reduces temperature
Chemical Combustion	Gas – Halon or Halon substitute	Interferes with the chemical reactions between elements

### **2.6.6** *Water Sprinklers*

Alat penyembur air bisa lebih sederhana dan tidak mahal dibandingkan sistem Halon, tetapi bisa mulai memyembur dari yang tidak seharusnya, yang menyebabkan kerusakan karena air. Jika kebakaran listrik dalam proses, air dapat menambah

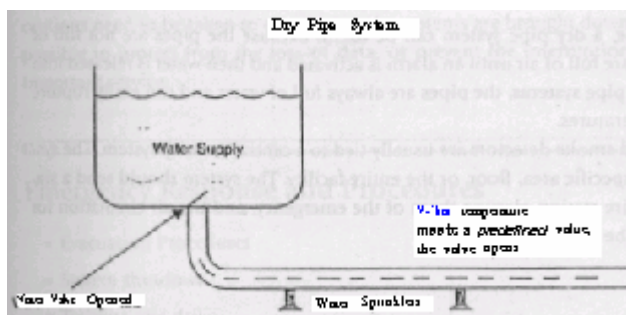
intensitas api, menyebabkan kerusakan yang lebih parah. Oleh sebab itu, perusahaan perlu memperhatikan dalam mengambil keputusan dimana paling baik sistem ini diterapkan

Sensor sebaiknya ditempatkan untuk men-*shutdown* aliran listrik sebelum *water sprinklers* diaktifkan. Masing-masing *sprinkler head* harus diaktifkan secara sendiri-sendiri untuk menghindari kerusakan area yang lebih luas dan harus ada katup *shutoff* sehingga suplai air bisa dihentikan jika perlu.

Ada empat tipe utama *sprinkler system* yang tersedia: *wet pipe*, *dry pipe*, *preaction*, dan *deluge*.

**Wet Pipe** *Wet pipe systems* selalu berisi air di pipa dan biasanya dikeluarkan oleh sensor tingkat pengawasan temperatur. Kalau temperatur mencapai tingkat yang ditentukan sebelumnya, jalurnya mencair, yang melepaskan air. Sistem ini sangat umum dan dipertimbangkan paling dapat diandalkan. Satu kerugian *wet pipe* adalah bahwa air di pipa mungkin membeku, yang dapat merusak pipa atau memberikan hasil yang kurang baik saat terjadi kebakaran. Juga, jika ada *nozzle* atau pipa yang rusak, bisa menyebabkan kerusakan karena air besar. Sistem seperti ini biasa disebut *closed head systems*.

**Dry Pipe** Pada *dry pipe system*, air tidak ditempatkan di pipa, tetapi dicegah oleh katup sampai suhu tertentu tercapai. Ada waktu tunda antara temperatur yang sudah mencapai tingkat yang ditentukan sebelumnya dan pengeluaran air. Ini bisa menjadi hal baik karena memberikan waktu bagi seseorang untuk menutup sistem walaupun terjadi alarm palsu, tetapi juga tidak bereaksi secepat sistem *wet pipe* lakukan, yang berarti memungkinkan terjadinya kerusakan yang besar sebelum sempat mengambil tindakan pencegahan. Sistem *Dry Pipe* ditunjukkan pada Gambar 2.7



**Gambar 2.7** Sistem *Dry Pipe* [3]

Air tidak dibolehkan masuk ke pipa yang akan disemburkan alat penyembur sampai alarm

kebakaran sebenarnya berbunyi. Pertama sensor panas atau asap diaktifkan, kemudian air mengisi pipa yang menuju ke alat penyembur, alarm kebakaran berbunyi, sumber daya listrik dilepaskan, dan segera air boleh mengalir dari alat penyembur. Pipa ini lebih baik digunakan di iklim yang dingin karena pipa tidak akan membeku.

**Preaction** *Preaction systems* menggabungkan penggunaan sistem pipa basah dan kering. Air tidak dimasukkan ke pipa dan hanya dilepaskan sekali ke dalam pipa saat temperatur mencapai batas yang ditentukan. Sekali temperatur tercapai, pipa diisi dengan air, tetapi tidak dilepaskan segera. Jalurnya dicairkan terlebih dahulu sebelum air dilepaskan dari kepala alat penyembur. Tujuan menggabungkan dua teknik ini agar dapat bereaksi lebih cepat terhadap alarm palsu atau kebakaran kecil yang bisa ditangani dengan cara lain. Jika kebakaran kecil terjadi, bisa dipadamkan dengan alat pemadam yang dipegang dengan tangan, ini akan lebih baik daripada merusak banyak perlengkapan listrik dari kerusakan karena air. Sistem ini biasanya dipilih untuk perlengkapan yang mahal dan kalau perusahaan mau mencegah kerusakan karena air.

**Deluge** *A deluge system* adalah sama seperti sistem pipa kering kecuali pada terbukanya kepala alat penyembur. Di sistem pipa kering kepala alat penyembur tertutup dan harus terbuka untuk membolehkan air mengalir. Di *deluge system*, kepala terbuka untuk membolehkan volume air yang lebih besar dilepaskan dalam periode waktu yang lebih pendek. Karena air yang dilepaskan volumenya besar, sistem seperti ini biasanya tidak digunakan di lingkungan pengolahan data.

Sistem pipa kering dipergunakan untuk melindungi kerusakan karena air dan dari alarm kebakaran palsu. Sebagai tambahan, kalau fasilitas di lokasi di mana temperatur membeku dan pipa rusak akan menjadi persoalan, sistem pipa kering sangat berguna karena pipa tidak penuh air. Pipa hanya penuh dengan udara sampai alarm diaktifkan lalu air dilepaskan ke dalam pipa. Di *wet pipe system*, pipa selalu penuh air dan mudah pecah pada saat temperatur beku.

Semua sensor dan detektor asap biasanya berhubungan dengan sistem keamanan pusat. Sistem bisa meliputi area tertentu, lantai, atau seluruh fasilitas yang ada. Sistem sebaiknya mengirimkan tanda peringatan ke pos pemadam kebakaran

lokal yang selalu siaga dalam keadaan darurat, dan sirkulasi udara di area tersebut harus di tertutup.

## **2.7 Pengawasan Administrasi (*Administrative Controls*)**

Pada dasarnya, pimpinan bertanggung jawab atas semua yang terjadi dalam perusahaan, dengan sedikit pengecualian. Manajemen yang baik harus mempunyai pandangan ke masa depan dan tahu bahwa beberapa hal mungkin diluar rencana, situasi tertentu yang perlu penanganan khusus, dan pegawai mungkin dihadapkan pada situasi keadaan darurat. Adalah tanggung jawab manajemen untuk memikirkan berbagai macam skenario, mengembangkan prosedur dan jawaban yang sebaiknya dilakukan bila terjadi situasi tertentu, dan merencanakan aktivitas *backup* dan kegiatan *contingency* untuk menjamin keberadaan perusahaan dan keamanan bagi setiap orang. Bagian selanjutnya akan menyinggung beberapa persoalan yang sama, tetapi menunjukkan seberapa dekat hubungannya dengan keamanan fisik.

### **2.7.1 *Emergency Response and Reactions***

Selama pengembangan rencana kelanjutan usaha dan penanggulangan bencana, skenario bencana yang berbeda dipersiapkan, situasinya di diperiksa/uji, dan keadaannya dipikirkan secara mendalam. Masalah keamanan fisik memerankan tugas yang sangat besar terutama bila hal tersebut benar-benar terjadi. Ada kontrol secara administratif yang perlu ditaruh pada tempatnya untuk menjamin bila bencana datang, orang-orang dapat bereaksi dengan semestinya. Kontrol administratif itu ialah: prosedur evakuasi, prosedur sistem *shutdown*, teknik pemadaman api, cara mengatasi ancaman bom dan kerusakan sipil, dan apa yang dilakukan jika utilitas tertentu gagal.

Rencana evakuasi perlu dikembangkan dan prosedur sistem *shutdown* dalam situasi keadaan darurat perlu dibentuk. Selama pengembangan rencana kesinambungan perusahaan, sistem yang menyimpan informasi penting akan diidentifikasi. Selama situasi keadaan darurat, sistem tersebut sebaiknya diperlakukan berbeda dengan *workstation* yang lain. Tindakan pencegahan perlu dilakukan untuk memastikan

bahwa sistem tetap terlindungi dari kemungkinan kehilangan data, atau mencegah gangguan dari layanan yang penting.

Utilitas yang *redundant* mungkin diperlukan untuk memberikan suplai daya bagi yang memerlukan bila ada kegagalan daya secara elektronik. Biaya UPS tergantung pada beban listrik yang dapat didukungnya, lamanya waktu yang bisa mendukung beban tersebut, dan kecepatan mengambil alih beban kalau sumber daya utama gagal. Jika suplai daya dibutuhkan dalam jangka panjang, kemungkinan pembangkit tenaga listrik diperlukan di tempat tersebut.

Prosedur keadaan darurat perlu di lakukan bila terjadi kebakaran, ancaman bom, angin ribut, angin tornado, dan kerusuhan sipil. Kalau bencana terjadi, setiap orang harus bertanggung jawab dan melakukan tugas tertentu. Pendelegasian setiap tugas juga terjadi selama masa rencana bisnis selanjutnya, latihan berkala, dan tugas-tugas yang harus dilakukan. Kegiatan tersebut sebaiknya dilakukan untuk menyelenggarakan setiap kebutuhan dari tugas tertentu. Manajemen bertanggung jawab untuk memastikan bahwa setiap pegawai telah dilatih untuk menanggulangi bencana dan prosedur kesinambungan perusahaan. Semua prosedur sebaiknya tercatat dan dokumentasi tersebut sebaiknya mudah didapat. Sebaiknya ada pemeriksaan secara berkala untuk memeriksa dokumentasi, prosedur, dan pengetahuan setiap orang apa yang diharapkan dari padanya. Perusahaan dan lingkungannya akan berubah secara berkesinambungan, dan oleh karena itu harus selalu diperhatikan akan terjadinya ancaman dan keringkahan.

Rencana penanggulangan sebaiknya menjadi sebuah dokumen yang secara terus-menerus diperiksa, diperbarui, dan dipraktekkan.

## ***2.8 Perimeter Security***

Hal utama terhadap penjagaan yang berhubungan dengan *perimeter control* adalah mencegah akses yang tak sah ke fasilitas tertentu. Penjagaan ini bekerja dalam dua mode utama: penerapan keamanan selama operasi dan keamanan selama waktu fasilitas tertentu ditutup. Saat fasilitas ditutup, semua pintu sebaiknya dikunci dengan

mekanisme pengawasan dalam posisi strategis untuk menyiagakan seseorang terhadap aktivitas yang mencurigakan.

Saat fasilitas beroperasi, keamanan menjadi lebih rumit karena setiap individu yang berhak harus dibedakan dari individu yang tidak berhak. *Perimeter control* berhubungan dengan pengawasan akses, memonitor penjagaan, deteksi penyusupan, dan tindakan korektif. Bagian berikut menjelaskan elemen yang membuat kategori-kategori tersebut.

### **2.8.1 Facility Access Control**

Standard pertama pada pengamanan fisik adalah fasilitas kontrol akses, yang memerlukan entiti yang meliputi: “Menerapkan kebijakan dan prosedur ke akses fisik terbatas ke perangkat elektronik dan fasilitas sistem informasi atau fasilitas dalam lingkup kerja, ketika memastikan hanya akses yang berhak yang diizinkan masuk.” Fasilitas didefinisikan dalam aturan “Benda-benda fisik dan interior dan eksterior dari gedung.”[2]

Kontrol akses perlu dilakukan dengan komponen fisik dan teknik kalau hal tersebut menjadi keamanan fisik. Kontrol akses melindungi fasilitas, komputer, dan orang. Di beberapa situasi, tujuan kontrol akses fisik dan perlindungan terhadap jiwa orang mungkin menjadi konflik. Dalam situasi ini, hidup seseorang selalu menjadi prioritas. Banyak kontrol keamanan fisik membuat jalan masuk dan keluar dari fasilitas menjadi sulit, bila tidak dikatakan mustahil. Namun bagaimanapun, perlu pertimbangan khusus bila hal tersebut berpengaruh terhadap jiwa seseorang. Kontrol keamanan fisik yang dipergunakan untuk menjamin bahwa seseorang yang bertujuan tidak baik jangan sampai diijinkan seperti orang yang bertujuan baik berada dalam situasi kebakaran atau tipe yang sama dalam keadaan darurat.

Kontrol akses fisik menggunakan mekanisme untuk mengenali individu yang sedang mencoba memasuki fasilitas, area, atau sistem. Untuk memastikan bahwa individu yang benar boleh masuk dan individu yang salah harus tetap diluar dan disediakan pemeriksaan tertentu terhadap aksi tersebut.

Dengan menempatkan orang di daerah yang peka bisa menjadi salah satu

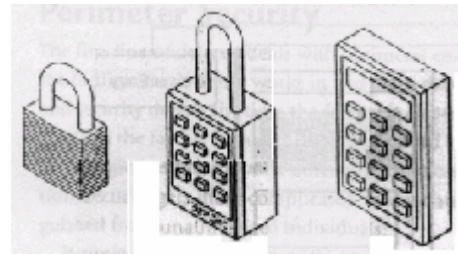
kontrol keamanan terbaik sebuah perusahaan karena secara pribadi mereka bisa mengetahui kelakuan yang mencurigakan; tetapi, mereka perlu dilatih atas aktivitas apa yang harus dicurigai dan bagaimana melaporkan aktivitas yang sebenarnya terjadi. Sebelum mekanisme perlindungan yang tepat ditempatkan, diperlukan analisa terperinci atas data yang peka dan memerlukan perlindungan, siapa yang dibolehkan ke area tertentu, yang mana ruang kerja dan sistem dipertimbangkan tingkat kritisnya terhadap misi perusahaan; dan bagaimana aliran data dan aliran kerja terjadi di dalam fasilitas tersebut. Titik kontrol akses akan dikenali dan digolongkan secara eksternal, utama, dan pintu masuk sekunder. Orang-orang diharapkan masuk dan keluar melalui tempat khusus agar bila masuk lewat jalan lain mudah dikenali. Yang penting terlebih dulu adalah menentukan apa yang perlu untuk dilindungi, kemudian langkah selanjutnya bagaimana melindunginya.

**Kunci** Kunci dan anak kunci adalah mekanisme kontrol akses yang paling murah. Kunci dianggap sebagai alat pencegah terhadap penyusup semi-serius dan alat penunda bagi pengacau serius. Semakin lama waktu yang diperlukan untuk memecahkan atau membuka kunci akan memberi waktu yang lebih panjang bagi seorang petugas keamanan atau polisi tiba di tempat jika penyusup sudah diketahui. Hampir semua tipe pintu dapat diperlengkapi dengan kunci, tetapi kunci dengan mudah bisa hilang dan digandakan, dan kunci bisa diambil atau rusak. Jika perusahaan bergantung semata-mata pada mekanisme *lock-and-key* untuk perlindungan, seseorang yang mempunyai kunci bisa datang dan pergi sesuka hatinya tanpa pengawasan dan dia bisa mengambil barang dari tempatnya tanpa terdeteksi. Kunci sebaiknya digunakan sebagai bagian dari skema perlindungan, tetapi tidak semata-mata digunakan sebagai skema perlindungan.

Ada bermacam-macam jenis kunci sesuai dengan fungsinya. Gembok bisa dipakai untuk pagar yang dirantai, *preset locks* biasanya digunakan pada pintu, dan kunci yang dapat diprogram (memerlukan kombinasi untuk membuka kunci) digunakan pada pintu *pushbutton* atau ruangan besi. Kunci terdiri dari banyak tipe

dan ukuran. Hal penting untuk memiliki tipe kunci yang tepat sehingga memberikan tingkat perlindungan yang benar. Berbagai jenis kunci ditunjukkan Gambar 2.8

**Gambar 2.8** Jenis-Jenis Kunci [3]



**Preset Locks** *Preset locks* biasanya digunakan pada pintu. Bisa berupa kombinasi *key-and-knob*, *mortise*, atau kunci yang melingkar dengan kancing/grendel dan *deadbolts* sebagai *needed*.

**Cipher Locks** *Cipher locks*, juga dikenal sebagai kunci yang dapat diprogram, menggunakan *keypads* untuk mengawasi akses ke dalam area atau fasilitas tertentu. Kunci memerlukan kombinasi spesifik yang dimasukkan ke dalam *keypad*, atau *swipe card*, atau kombinasi dari keduanya. Biayanya jelas lebih mahal daripada kunci tradisional, tetapi kombinasi dapat diubah, kombinasi khusus untuk *locked out*, dan orang yang mengalami kesulitan atau memaksa untuk masuk dengan kode tertentu dapat membuka pintu dan membunyikan alarm jarak jauh pada saat bersamaan. Jadi, *cipher lock* memberikan tingkat pengawasan dan keamanan yang lebih tinggi terhadap orang yang dapat mengakses fasilitas tertentu dibandingkan dengan kunci tradisional.

Berikut adalah beberapa pilihan yang tersedia untuk *cipher lock* yang meningkatkan kinerja kontrol akses dan memberikan tingkat keamanan yang lebih baik:

- *Door delay* bila pintu terbuka untuk jangka waktu lama, alarm akan dipicu untuk memperingatkan orang-orang bahwa ada aktivitas yang mencurigakan.
- *Key override* kombinasi khusus yang dapat diprogram untuk digunakan dalam situasi darurat untuk mengesampingkan prosedur standar atau untuk mengesampingkan pengawasan.
- *Master-key* pilihan ini memungkinkan seorang pengawas berganti kode akses dan fitur lain dari *cipher lock*.

- *Hostage alarm* Jika seorang dipaksa dan/atau disandera, ada kombinasi yang dapat ia masukkan dalam situasi ini untuk berkomunikasi dengan pos penjaga dan/atau kantor polisi.

Jika pintu dilengkapi dengan *cipher lock*, sebaiknya mempunyai perisai visibilitas agar seorang yang berada disisi lain tidak bisa melihat kombinasi saat diketik.

*Cipher lock* yang otomatis harus mempunyai sistem batere cadangan dan diset untuk *unlock* selama kerusakan listrik sehingga pegawai tidak terjebak di dalam area selama keadaan darurat.

**Device Locks** Sayangnya, perangkat keras cenderung bergerak meninggalkan fasilitas; oleh karena itu, perangkat kunci kadang-kadang perlu dihalangi dari hal tersebut. Kabel kunci terdiri dari baja yang dilapisi *vinyl* yang memungkinkan komputer dan perlengkapannya dapat dijangkarkan ke meja tulis, kursi, dan bagian yang tak bergerak lainnya.

Berikut dijelaskan beberapa perbedaan tipe perangkat kunci yang tersedia dan kemampuannya:

- *Switch controls* menangani switch daya on/off.
- *Slot locks* sebuah siku-siku diletakkan di *spare expansion slot* dan kabel baja digunakan untuk mengamankan sistem ke bagian yang tak bergerak.
- *Port controls* menghalangi akses ke *disk drives*, port serial atau port paralel yang tidak digunakan.
- *Peripheral switch control* mengamankan keyboard dari penekanan switch on/off diantara unit sistem dan slot masukan keyboard.
- *Cable traps* mencegah pemindahan perangkat input/output dengan menempatkan kabel-kabelnya melewati unit yang dapat dikunci.

### **2.8.2 Personnel Access Control [4]**

Identifikasi yang tepat perlu dilakukan untuk mencek bila seseorang mencoba mengakses fasilitas atau area yang diperbolehkan. Identifikasi bisa dilakukan dengann mengenali sifat anatomis (sistem biometric), *smart* atau *memory card (swipe*

*cards*), penandaan pribadi oleh seorang petugas keamanan dan memberikan foto ID, menggunakan kunci, atau memberikan kartu dan memasukkan *password* atau PIN. Masalah umum yang terjadi dengan mengawasi akses secara sah ke dalam fasilitas atau area disebut *piggybacking*. Hal ini terjadi kalau seorang individu mendapat akses yang tak sah dengan memakai hak akses orang lain. Biasanya seorang individu hanya menyusul orang lain secara lebih dekat melewati pintu dengan tidak memberikan surat kepercayaan yang mana pun. Tindakan pencegahan terbaik terhadap masalah ini adalah petugas keamanan dan pegawai dididik dengan latihan keamanan yang baik. Jika perusahaan menerapkan *card badge reader*, ada beberapa tipe sistem yang dapat dipilih. Kartu magnetik dapat berisi sebuah *magnetic strip*, berisi informasi otorisasi, titik magnetik, *embedded wire (resists tampering)*, atau *proximity card*, yang berarti tidak perlu di-*swipe* lewat *reader*, tetapi kamera di atas pintu dapat membaca kartu saat seseorang mendekatinya.

### **Magnetic Cards**

Seseorang mempunyai kartu yang sudah memasukkan *magnetic strip* yang berisi informasi akses. *Reader* hanya melihat informasi akses yang sederhana didalam *magnetic strip* atau bisa dihubungkan ke sistem yang lebih canggih yang dapat men-*scan* informasi, membuat keputusan akses yang lebih kompleks, logs kartu ID dan waktu akses.

Jika kartu adalah *memory card*, lalu *reader* hanya akan menarik informasi darinya dan membuat keputusan akses. Jika kartu adalah *smart card*, seseorang mungkin diharuskan memasukkan PIN atau *password*, yang akan dibandingkan dengan informasi yang berada di dalam kartu.

### **Wireless Proximity Readers**

Tidak seperti penerapan *swipe card*, *proximity reader* tanpa kabel tidak mengharuskan seseorang memasukkan kartu ke dalam *reader*. *Reader* dapat merasakan kartu pada jarak tertentu dan membuat keputusan akses. Dua tipe dari *proximity reader* adalah *user activated* dan *system sensing*.

**User Activated** Ketika tipe *reader* ini digunakan, *proximity card* meneruskan urutan nilai kepada *reader*. *Reader* mengharapkan urutan yang spesifik dan jika apa yang dikirim sama dengan nilai yang diset, maka seseorang diberi akses.

**System Sensing** Pada sistem jenis ini, *system-sensing proximity card* akan mengenal adanya alat bersandi dalam area tertentu. Sistem kontrol akses *system-sensing* adalah alat yang tidak mengharuskan seseorang memasukkan urutan apapun atau melakukan tindakan yang mana pun. Gambar 2.9 menunjukkan bagaimana *reader* dapat memproses kartu dan mengirim kode ke *authentication server*, yang kemudian membuat keputusan akses.

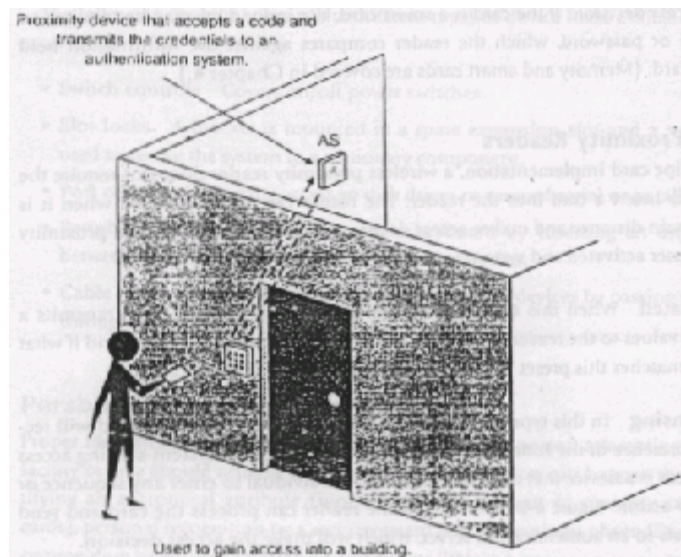
**Gambar 2.9** Kartu berkomunikasi dengan proximity reader untuk memberikan akses [3]

Ada tiga tipe utama dari sistem *sensing cards* dan perbedaan diantara mereka berdasarkan pada bagaimana cara membangkitkan dayanya.

- **Transponders Card** dan *reader* memiliki *receiver*,

*transmitter*, dan baterai. *Reader* mengirim sinyal ke *card* untuk meminta informasi. *Card* mengirim ke *reader* sebuah kode akses. Perangkat *transponder* berisi *radio receiver* dan *transmitter*, tempat penyimpanan kode akses, *control logic*, dan baterai.

- **Passive devices Card** dianggap pasif karena tidak memiliki sumber daya bila *down*, tetapi menggunakan daya dari *reader*. Bilapun perangkat ini pasif, *card* dapat merasakan medan elektromagnetik, yang ditransmisikan oleh *reader*. Saat seseorang sudah berada di area yang aman dan mendekati pintu untuk meninggalkan area yang peka ke area yang tidak begitu peka, *reader* akan mendeteksi keberadaan *card* dan segera membuka pintu.



- **Field-powered devices**      *Card* dan *reader* berisi *transmitter* dan elektronik aktif. *Card* memiliki suplai daya sendiri dan tidak mengandalkan suplai daya dari *reader*.

### **2.8.3 External Bondary Protection Mechanisms**

Ada beberapa tipe mekanisme perlindungan dan pengawasan yang dapat digunakan untuk melindungi fasilitas perusahaan. Yang dapat mendeteksi seorang penyusup dan kegiatan yang tidak biasa, dan dapat memberikan cara mengatasi persoalan bila masalah tersebut terjadi. Perbedaan mekanisme dan pengawasan dijelaskan di bagian berikut.

#### ***Fencing***

*Fencing* adalah rintangan fisik yang cukup efektif karena bekerja sebagai pencegah dan mekanisme pencegahan. *Fencing* bisa menyediakan pengawasan terhadap orang banyak dan membantu kontrol akses di pintu masuk dan akses ke fasilitas. Tetapi, *fencing* mahal dan mengganggu pemandangan. Banyak perusahaan menanam rumput atau pohon di sekitar pagar untuk melindungi gedung mereka secara estetika dan memungkinkan gedung kurang kelihatan.

Pagar memiliki tinggi yang bervariasi dan dari tingginya memberikan tingkat keamanan yang berbeda pula:

- pagar dengan tinggi hanya tiga sampai empat kaki hanya menghalangi pelanggar yang sambil lalu.
- pagar dengan tinggi enam sampai tujuh kaki dianggap terlalu tinggi untuk dipanjat dengan mudah.
- pagar dengan tinggi delapan kaki serta ditambah kawat berduri berarti anda serius untuk melindungi milik anda. Ini akan menghalangi penyusup yang lebih gigih.

Area yang kritis seharusnya mempunyai pagar dengan tinggi sedikitnya delapan kaki untuk memberikan tingkat perlindungan yang semestinya.

#### ***Lighting***

*Lighting* sebaiknya dipergunakan untuk menciutkan hati penyusup dan memberikan keamanan bagi orang, pintu masuk, lapangan parkir, dan bagian yang kritis. *Lighting* adalah pengawasan fisik yang disediakan untuk mencegah penyusup.

Perusahaan harus menyediakan tipe *lighting* yang benar untuk area yang dipertimbangkan berbahaya. Misalnya, jika seorang pegawai diserang di tempat parkir perusahaan, pegawai itu bisa menuntut perusahaan karena tidak memberikan keamanan yang semestinya. Jika perusahaan tidak mengambil tindakan untuk menjamin lingkungan aman bagi pegawainya, maka perusahaan dianggap lalai dan mungkin kalah dalam perkara pengadilan.

### ***Surveillance Devices***

Biasanya memasang pagar dan memasang lampu tidak selalu memberikan tingkat perlindungan yang dibutuhkan perusahaan untuk melindungi fasilitas, perlengkapan, dan pegawainya. Area tertentu perlu diawasi agar tindakan tidak patut bisa diperhatikan dan diselesaikan sebelum kerusakan terjadi. Pengawasan bisa dilakukan lewat deteksi visual atau teknologi yang memakai alat canggih yang dapat mengetahui tindakan yang tidak normal atau kondisi yang tidak diinginkan. Tiga kategori pengawasan utama adalah petugas keamanan, anjing, dan alat perekam visual.

***Patrol Force and Guards*** Salah satu mekanisme keamanan terbaik adalah seorang petugas keamanan dan/atau *patrol force* (patroli angkatan perang) untuk mengamati fasilitas. Kontrol keamanan jenis ini lebih fleksibel daripada mekanisme keamanan yang lain, karena memberikan *response* yang baik terhadap aktivitas yang mencurigakan, dan bekerja sebagai alat pencegah yang terbaik. Tetapi, bisa menjadi berbiaya mahal, karena memerlukan gaji, keuntungan, dan waktu istirahat. Kehandalan seseorang itu biasanya terbatas dalam waktu tertentu. Seleksi dan *bonding* adalah bagian yang penting saat memilih seorang petugas keamanan, tetapi inilah satu-satunya yang dapat memberikan tingkat kepastian yang sebenarnya.

Sistem deteksi gangguan (*intrusion detection system*) dan ukuran perlindungan fisik pada akhirnya memerlukan campur tangan manusia. Petugas keamanan bisa ditempatkan di pos tertentu atau melakukan ronda yang meliputi area spesifik. Organisasi berbeda akan memerlukan petugas keamanan yang berbeda pula. Mereka mungkin diharuskan memeriksa tanda pengenalan setiap orang dan mengharuskan untuk mengisi log kehadiran ataupun ketika akan keluar/pulang, mereka mungkin

bertanggung jawab untuk mengamati sistem deteksi gangguan dan diharapkan bertindak bila ada alarm, mereka mungkin perlu membuat dan mengambil kartu tanda pengunjung/tamu, bertindak terhadap alarm kebakaran, menyelenggarakan peraturan yang diterapkan oleh perusahaan didalam gedung, dan mengontrol semua material yang masuk atau keluar area. Penjaga mungkin perlu untuk mengecek bahwa pintu, jendela, peti besi, dan ruangan besi sudah dilindungi; membuat laporan bahaya keamanan; membuat pembatasan terhadap area yang sensitif; dan mendampingi seseorang selama berada di dalam fasilitas.

Untuk perusahaan yang berskala UKM mungkin seorang atau dua orang petugas keamanan sudah cukup untuk mengawasi aset perusahaan.

**Dogs** Anjing terbukti sangat berguna dalam mengetahui penyusup dan kondisi yang tak diinginkan lainnya. Kemampuan pendengaran dan penglihatannya mengungguli manusia dan kecerdasan serta kesetiiaannya dapat digunakan sebagai ukuran perlindungan. Anjing sebagai keamanan terbaik harus dilatih agar mereka mempunyai tingkat pemahaman yang tinggi terhadap perintah yang diberikan. Anjing bisa dilatih untuk menangkap seorang pengacau sampai seorang satpam tiba atau mengejar seorang pengacau dan menyerangnya. Beberapa anjing terlatih mengenali asap sehingga mereka bisa menyiagakan orang lain terhadap kebakaran yang terjadi. Tentu saja, anjing tidak selalu bisa membedakan antara orang yang berwenang dan orang yang tak berwenang, oleh sebab itu jika seseorang masuk kerja sesudah jam kerja selesai, dia bisa mempunyai lebih banyak kesempatan daripada yang diharapkan. Anjing bisa sebagai suplemen yang baik terhadap mekanisme keamanan, atau perusahaan bisa bertanya kepada petugas keamanan untuk menunjukkan giginya yang dapat dilihat apakah seseorang dikenal atau tidak dikenal.

**Visual Recording Devices** Karena pengawasan berdasarkan persepsi sensor/ indra, alat pengawasan biasanya bekerja bersama dengan penjaga untuk meningkatkan kemampuan dan tingkat persepsi mereka. Kamera bisa dipergunakan untuk mengambil gambar fotografis, yang disimpan untuk dilihat kemudian atau perusahaan bisa memilih untuk menggunakan *closed-circuit TVs* (CCTVs). CCTV memungkinkan seorang penjaga mengamati banyak area berbeda sekaligus dari satu

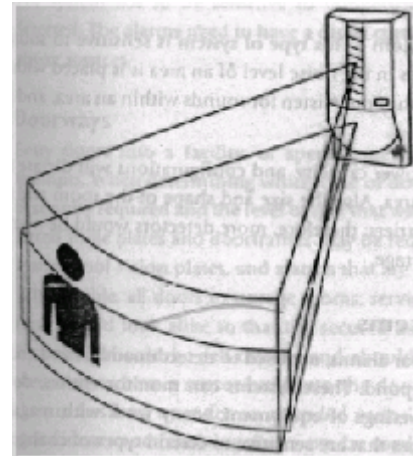
tempat. Area yang kritis mungkin memerlukan tingkat perlindungan lain untuk menjamin bahwa area ini memang kosong selama libur atau selesai jam kerja.

### ***Detecting***

Teknik pengawasan digunakan untuk mengawasi tindakan yang tidak biasa, sedangkan alat pendeteksi digunakan untuk merasakan adanya perubahan di sekitar lingkungan. Keduanya merupakan metode pengawasan, tetapi menggunakan alat dan pendekatan yang berbeda. Bagian berikut menjelaskan teknologi yang bisa dipergunakan untuk mengetahui adanya seorang pengacau/penyusup. Contoh tipe perangkat *perimeter scanning* ditunjukkan oleh

Gambar 2.10

**Gambar 2.10** Perangkat *perimeter scanning* bekerja melingkupi area tertentu [3]



### ***Proximity Detection System*** *proximity*

*detector*, atau *capacitance detector*, memancarkan medan magnet yang dapat diukur saat digunakan. Detektor mengamati medan listrik dan alarm berbunyi jika medannya diganggu. Alat ini

biasanya dipergunakan untuk melindungi benda tertentu (karya seni, lemari kaca, atau peti besi) tetapi tidak melindungi seluruh ruangan atau area secara utuh.

***Photoelectric atau Photometric System*** sistem jenis ini mendeteksi perubahan kadar cahaya dalam area, dan biasanya harus digunakan di ruangan tanpa jendela. Sistem ini bekerja seperti *photoelectric smoke detectors*, yang memancarkan bias cahaya dan diharapkan mengaktifkan *receiver*. Bila bias cahaya ini terganggu, alarm berbunyi. Bias cahaya dipancarkan oleh sel *photoelectric* secara menyilang dan bisa terlihat atau tidak terlihat.

***Wave Pattern*** Detektor pola gerakan gelombang dengan tingkat berbeda pada frekuensi gelombang, dapat diketahui. Perbedaan frekuensi itu adalah *microwave*, ultrasonik, dan frekuensi yang rendah. Semua alat ini menyebabkan timbulnya pola gelombang yang dikirim melalui area yang sensitif dan memantul kembali ke

*receiver*. Jika pola yang dikembalikan tidak terganggu, alat tidak bereaksi apa-apa. Jika pola yang kembali berubah, alarm akan berbunyi.

***Passive Infrared System*** sistem jenis ini mengidentifikasi perubahan gelombang panas dengan area yang dikonfigurasi untuk dilindungi. Jika partikel di udara mengalami peningkatan, bisa menjadi tanda adanya seorang penyusup.

***Acoustical-Seismic Detection System*** sistem jenis ini peka terhadap bunyi dan getaran dan mendeteksi perubahan tingkat kebisingan dari area dimana dia ditempatkan. Alat ini tidak memancarkan gelombang apapun; mereka hanya memperhatikan bunyi di dalam area, dan dianggap sebagai alat yang pasif.

Jenis dari *motion detector*, berkapasitas daya, dan konfigurasi akan memberikan sejumlah perintah yang diperlukan untuk melingkupi area yang peka. Juga ukuran dan bentuk dari ruangan dan item didalam ruangan dapat mengakibatkan adanya rintangan; oleh karena itu, diperlukan lebih banyak detektor untuk memberikan cakupan yang lebih baik.

#### **2.8.4 *Intrusion Detection Systems***

Sistem deteksi penyusupan, atau alat tanda bahaya, digunakan untuk mendeteksi sesuatu yang tidak diizinkan masuk dan peringatan untuk bertanggung jawab memberikan respon. Sistem tersebut dapat memonitor pintu, jendela, perangkat, atau peralatan yang dapat berpindah. Kebanyakan bekerja dengan kontak magnet atau perangkat deteksi getar yang sensitif untuk memastikan tipe perubahan lingkungan sekitar. Saat dideteksi ada perubahan, alarm akan berbunyi di area lokal, atau di area lokal dan tempat penjaga atau kantor polisi.

Tipe IDS yang paling populer yang digunakan saat ini adalah tipe elektromagnetik yang mendeteksi perubahan atau memutus rangkaian. Rangkaian listrik dapat dililit dengan foil terpasang atau dihubungkan ke jendela. Bila jendela rusak, kepingan foil akan putus, kemudian alarm berbunyi. Pendeteksi getar akan mendeteksi perpindahan di dinding, langit-langit, dan lantai ketika kabel yang terpasang di dalam struktur rusak. Switch kontak magnetik dapat diinstal pada jendela

dan pintu. Jika kontak tersentuh karena jendela atau pintu terbuka, alarm akan berbunyi.

Apa perbedaan diantara pendeteksi kedekatan (*proximity detector*), deteksi seismik (*seismic detector*), deteksi getar (*vibration detector*), dan deteksi penyusup (*intrusion detector*)? Deteksi seismik dan getar, keduanya merasakan getar atau pergerakan dan menginterpretasikan hal ini sebagai gangguan fisik dan membunyikan alarm. *Detector proximity* dapat merasakan suatu objek atau individu yang masuk ke area yang dilindungi dan menganggap hal tersebut sebagai serangan dan alarm akan berbunyi. Sistem pendeteksi penyusup dikonfigurasi untuk mendeteksi individu atau objek yang melintas garis atau masuk ke area, dan kemudian memulai alarm.

Deteksi gerakan, lampu sorot, dan sensor getar sangat mahal untuk diinstal dan dimonitor. Bila alarm berbunyi, membutuhkan tanggapan dari manusia. Mereka cenderung mengaktifkan alarm walaupun tidak ada penyusup atau percobaan penembusan. Perangkat pendeteksi tersebut dapat ditembus dan tidak diharapkan untuk disediakan terhadap keperluan keamanan dari semua fasilitas.

Tipe penyusupan api, dan detektor gerakan biasanya tidak terpisah, tetapi merupakan bagian dari sistem alarm. Semua sistem alarm memerlukan daya listrik yang konstan, dan sering sekali cara penyusup mencoba berada di sekitar sistem kemudian menghilangkan sumber daya listriknya. Sistem itu memiliki sensitif terhadap kerusakan dan membunyikan alarm bila kerusakan terdeteksi. Alarm butuh sumber daya listrik langsung dan sumber daya cadangan saat terjadi keadaan darurat.

### ***Doorways***

Pintu masuk ke dalam fasilitas, atau area khusus, sebaiknya dapat menolak percobaan masuk secara paksa. Ketika menentukan tipe pintu yang mana yang akan dibeli dan diimplementasikan, tingkat keamanan yang diperlukan dan tingkat risiko yang dapat diterima perlu dipertimbangkan. Memperkuat *strike plate* dan rangka pintu mungkin diperlukan sebagaimana dengan *tamper-resistant hinges*, *shatterproof vision plates*, dan alarm yang dapat dipicu bila ada pemaksaan.

Jika mungkin, semua pintu ke ruang penyimpanan, ruang perlengkapan, dan area yang diamankan harus tertutup rapat-rapat sehingga tidak menjadi perhatian. Setiap

pintu sebaiknya dapat menutup sendiri dan sebaiknya tidak memiliki palka-pembuka. Lebih baik mempunyai sensor yang dipasang pada rangka pintu untuk mengindikasikan ketika pintu tidak tertutup atau telah terbuka untuk periode waktu tertentu. Pintu putar atau pintu yang tetap dapat digunakan sebagai mekanisme pengawasan akses secara fisik. Dipakai untuk mencegah seseorang yang tidak berhak untuk memasuki fasilitas dan tidak bisa keluar bila diaktifkan. *Mantraps* melindungi akses fisik dengan mengarahkan seseorang melewati seorang petugas keamanan dan melewati area pintu ganda di mana seseorang sebagai subyek untuk selanjutnya diidentifikasi dan diotentikasi.

*Doorways* dengan kunci otomatis bisa dikonfigurasi sebagai *fail-soft* atau *fail-safe*. Setting *failsoft* berarti bahwa bila ada gangguan daya listrik, yang akan mempengaruhi sistem pengunci otomatis, pintu secara default akan tidak terkunci. Konfigurasi *fail-safe* berarti bahwa pintu akan secara default terkunci jika ada masalah dengan daya listrik. Perusahaan perlu memutuskan mana yang paling diperlukan.

### **BAB III**

### **KESIMPULAN**

Dengan jaringan yang tersebar, maka prosedur dan administrasi pengawasan menjadi tanggung jawab pemakai dan orang-orang jaringan, dibandingkan dengan mainframe dimasa lalu.

Keamanan fisik tidak hanya sekedar penjaga malam yang keluar untuk mengawasi area dengan lampu senter besar. Saat ini, keamanan sudah lebih bersifat teknik, terdapat dalam semua bentuk, dan meningkatkan banyak tanggungjawab dan persoalan hukum. Bencana alam, kebakaran api, banjir, penyusup, perusak, persoalan lingkungan, material konstruksi, dan persediaan daya listrik adalah semua hal yang harus direncanakan dan dikenal sedari awal.

Keamanan fisik sering tidak terpikirkan ketika seseorang berpikir masalah keamanan terutama untuk usaha kecil menengah (UKM), tetapi ada ancaman dan risiko nyata yang perlu diwaspadai dan direncanakan.

## DAFTAR ACUAN

- [1] <http://www.educause.edu/ir/library/pdf/DEC0305.pdf>  
[14 September 2005 02:23 PM]
- [2] [http://www.hipaadvisory.com/regs/finalsecurity/cms\\_papers/PhysicalSafeguards.pdf](http://www.hipaadvisory.com/regs/finalsecurity/cms_papers/PhysicalSafeguards.pdf) [14 September 2005 08:25 AM]
- [3] Harris, Shon, *CISSP All-in-One Certification Exam Guide*, McGraw-Hill, 2002
- [4] Krutz, Ronald L. & Russell Dean Vines, *The CISSP Prep Guide: Gold Edition*, Wiley Publishing Inc., 2003