Keamanan Fisik Teknologi Informasi: Desain Lingkungan

Hadi Prasetyo Utomo dan Awan Setiawan
Universitas Langlangbuana
Jalan Karapitan No.116 Bandung
e-mail: hadibanoe@live.com

Abstrak

Keamanan fisik fasilitas teknologi informasi menjadi semakin populer beberapa tahun belakangan ini. Hal ini disebabkan oleh semakin meningkatnya kesadaran institusi teknologi informasi terhadap pentingnya keamanan fasilitas fisik mereka. Keamanan fisik mempunyai cakupan yang sangat luas, meliputi hak akses, lingkungan dan juga infrastruktur. Banyak institusi tidak mempunyai pilihan dalam membangun keamanan fisiknya sendiri. Karena mayoritas infrastuktur yang digunakan merupakan infrastruktur yang sudah siap pakai. Hal ini tentu saja sangat membatasi kebijakan keamanan fisik yang ingin diterapkan. Selain aspek infrastruktur, ada aspek lain yang sering terabaikan, yaitu manusia yang terlibat di dalamnya. Manusia dapat melakukan kejahatan dengan berbagai kondisi. Maka dari itu, keamanan fisik juga harus mempertimbangkan motif dan situasi yang dapat memicu terjadinya kejahatan oleh manusia. Bahkan orang yang sangat dipercayapun mampu melakukan kejahatan jika motif dan situasinya mendukung. Dalam tulisan ini akan dibahas beberapa alternatif penanganan keamanan fisik berdasarkan CPTED (Crime Prevention Through Environmental Design) serta standarisasi infrastruktur berdasarkan TIA-942. Konsep dasar dari CPTED adalah bahwa lingkungan fisik dapat diubah dan berdampak pada berkurangnya tindak kejahatan. CPTED berfokus pada empat area untuk mencapai tujuannya, yaitu pengendalian akses, pengawasan pasif, kegiatan pendukung, dan motivasi. Sedangkan TIA-942 adalah standar yang dikeluarkan oleh Telecommunications Industry Association untuk infrastruktur teknologi informasi.

Kata kunci: *keamanan, fisik, CPTED, infrastruktur*

1. Pendahuluan

Banyak hal yang telah dilakukan oleh individu/organisasi dalam menjaga keamanan informasi yang mereka miliki. Mulai dari membuat *password* yang sulit ditebak, sistem deteksi penyusup, konfigurasi *firewall* dan *router*, *update* anti virus, *upgrade* sistem operasi, dan *backup* secara berkala. Semuanya dilakukan guna melindungi data dari penyusup yang dapat mencuri atau memanipulasi data yang terdapat pada sistem. Teknik pencegahan di atas dapat menjaga keamanan informasi dari sisi media elektronik. Akan tetapi ancaman yang terjadi bukan hanya dari sisi itu saja. Sebagian pengguna komputer kurang menyadari bahwa pelaku kejahatan dapat menggunakan berbagai cara untuk memperoleh akses ke sistem, baik dengan cara yang langsung seperti pencurian fisik, atau pun dengan cara tak langsung seperti rekayasa sosial.

Mayoritas orang bergantung pada perangkat media elektronik untuk memenuhi kebutuhan keamanan informasi mereka. Sebagai contoh, sebuah IDS memang dapat mendeteksi seseorang yang ingin menyerang sebuah *server*, tapi alat ini tidak dapat mengetahui jika ada orang yang masuk ke ruang *server*. Jika seseorang mempunyai akses fisik ke sebuah *server*, maka orang tersebut mempunyai kendali terhadap sistem dan data di dalamnya.

Fakta di atas dapat menyadarkan kita bahwa keamanan secara elektronik hanya sebagian kecil saja dari kebutuhan keamanan informasi secara keseluruhan. Untuk itulah keamanan secara fisik menjadi hal yang perlu dipertimbangkan secara serius. Karena dengan mengimplementasikan keamanan fisik, metode keamanan lainnya dapat diterapkan lebih efektif dan menjadi syarat mutlak untuk perencanaan keamanan informasi secara komprehensif [1].

Tulisan ini akan membahas bagaimana mencegah terjadinya kejahatan dalam sebuah institusi dengan metode CPTED (*Crime Prevention Through Environmental Design*). Menurut Cook [2], CPTED memiliki konsep yang menyatakan bahwa lingkungan fisik yang didesain sedemikian rupa dapat mencegah terjadinya tindak kejahatan. Masih menurut Cook [2], dengan berkurangnya kejahatan, kualitas sebuah institusi akan semakin terjaga dan akan meningkatkan kualitas hidup para pekerjanya. Akan dibahas juga bagaimana standarisasi infrastruktur berdasarkan TIA-942 dan hal-hal yang harus dilakukan guna infrastruktur teknologi informasi yang dimiliki dapat yang sesuai dengan standar yang ada.

2. Metode Penelitian

Dalam pelaksanaan penelitian ini penulis menggunakan metode pengumpulan data sebagai berikut :

2.1. Observasi Lapangan

Oberservasi ini dilakukan untuk mendapatkan gambaran situasi dan kondisi objek penelitian saat ini yaitu kampus utama Universitas Langlangbuana. Kegiatan ini juga berfungsi untuk mengetahui data primer yang dapat digunakan sebagai acuan awal penelitian.

2.2. Wawancara

Wawancara dilakukan terhadap pihak-pihak yang terkait dengan pengelolaan sumber daya untuk mendapatkan gambaran standar dan prosedur pengelolaan sumber daya saat ini.

2.3. Studi Kepustakaan

Studi kepustakaan ini dimaksudkan untuk pengumpulan dan memperoleh data sekunder dengan cara mempelajari, membaca dan mencatat literatur dari beberapa buku dan sumber yang berkaitan dengan permasalahan di atas.

3. Hasil dan Pembahasan

Pada bagian ini akan dibahas mengenai hal-hal yang berkaitan dengan Desain Fisik Teknologi Informasi dan CPTED seperti: aspek pekerja, aspek lingkungan dan standarisasi infrastruktur.

3.1. Aspek Pekerja

Ada dua macam sumber ancaman terhadap keamanan informasi, dari internal dan eksternal. Pekerja merupakan sumber internal, sedangkan orang di luar pekerja merupakan sumber eksternal, termasuk mantan pekerja. Pekerja harus mendapat perhatian yang serius dalam setiap perencanaan keamanan. Karena mayoritas kasus pencurian/pembobolan institusi berasal dari pekerja internal.

3.1.1. Motif

Banyak alasan mengapa mereka melakukan kejahatan tersebut. Dengan lebih memahami alasan-alasan tersebut, maka kita akan lebih mudah merancang keamanan informasi yang sesuai dengan kebutuhan institusi. Menurut Walsh [4], berikut adalah beberapa alasannya.

- Moral yang rendah: pekerja menjadi termotivasi untuk melakukan kejahatan karena mereka merasa tidak akan pernah naik karirnya dalam institusi.
- Merasa diperlakukan tidak adil: pekerja akan berusaha membalas dendam terhadap institusi dengan memanfaatkan hak akses yang dimiliki untuk melakukan kejahatan.
- Upah yang kurang layak: pekerja yang merasa pendapatannya tidak sebanding dengan kontribusi mereka pada institusi akan termotivasi untuk mencuri guna menutupi defisitnya.
- Konsekuensi yang ringan: pekerja merasa jika mereka melakukan pencurian tidak ada berdampak signifikan terhadap institusi. Misalnya sudah pernah ada kasus pencurian dan hukuman yang diterima si pencuri sangat ringan.
- Hutang dan pengeluaran: pekerja yang mempunyai banyak hutang dan pengeluaran yang lebih besar daripada pendapatannya akan termotivasi untuk mencuri agar dapat bertahan hidup secara ekonomi.
- Mata-mata: pekerja mungkin saja dibayar oleh institusi pesaing untuk mencuri informasi ataupun perangkat vital institusi.
- Peluang: banyak kejahatan terjadi tanpa alasan apapun selain adanya peluang. Pekerja yang belum pernah mencuri pun akan berani mencobanya jika ada peluang yang memungkinkan sebuah kejahatan tidak akan pernah diketahui oleh pihak institusi.

3.1.2. Solusi

Setelah diketahui alasannya, tindakan pencegahan dapat dilakukan sejak awal rekrutmen. Pemeriksaan riwayat kriminal calon pekerja menjadi hal yang sangat perlu dilakukan. Jangan sampai kita merekrut orang yang salah. Terlebih untuk posisi yang membutuhkan kejujuran dan kerahasian. Pada saat wawancara juga sebaiknya dibahas mengenai kebijakan yang terkait dengan tindak kriminalitas dalam institusi. Jadi calon pekerja akan mengetahui bahwa ada suatu peraturan mengikat dalam institusi

mengenai penanganan tindakan kriminalitas, yang mana peraturan tersebut mengikat seluruh tingkatan pekerja tanpa pandang bulu [4].

Untuk kasus dengan motif hutang, pekerja harus diyakinkan bahwa institusi tempatnya bekerja dapat membantu permasalahannya. Penanganannya dapat dilakukan dengan memberikan pinjaman lunak kepada pekerja. Kebijakan ini harus diatur dengan jelas dalam peraturan institusi, sehingga ada batasan-batasan yang jelas mengenai besarnya pinjaman dan aturan pengembaliannya [4]. Sedangkan untuk kasus moral yang rendah dan merasa tidak diupah dengan layak, penanganannya tak semudah kasus yang lainnya. Karena persoalan moral dan kelayakan merupakan hal yang tidak dapat diukur secara pasti. Ukuran seseorang dianggap bermoral serta ukuran kelayakan upah sangat relatif bagi setiap individu. Solusi yang paling baik untuk permasalahan ini adalah dengan membangun budaya institusi yang kondusif. Institusi harus dapat membangun rasa memiliki dan mengakui peran penting pekerja dalam institusi [4]. Dengan begitu, pekerja akan merasa dihargai dan berperan penting dalam institusi. Sehingga komunikasi antar sesama pekerja serta antar pekerja dan pemilik institusi dapat terjalin dengan harmonis. Dan yang paling penting dari semua hal di atas adalah bagaimana caranya mengurangi peluang yang ada. Pembatasan peluang merupakan tindakan yang paling efektif untuk mencegah terjadinya tindak kriminalitas dalam institusi. Solusinya dengan cara menerapkan pengawasan yang ketat, inventarisasi, dan audit secara berkala [1]. Periode audit pun harus dilakukan secara acak, sehingga pekerja tidak mengetahui jadwal yang pasti kapan audit akan dilakukan.

Pencegahan juga dapat dilakukan dengan memberikan pengetahuan kepada pekerja tentang hal-hal apa saja yang masuk kategori pencurian. Karena banyak pekerja yang melakukan pencurian, tetapi tak mengetahui bahwa yang dilakukannya adalah salah [4]. Misalnya menggunakan telepon kantor untuk kepentingan pribadi dan lain sebagainya. Jika pekerja merasa bahwa yang dilakukannya tidak menyalahi aturan, maka hal tersebut akan terus terjadi dan terjadi lagi. Bahkan dapat meningkat ke penggunaan fasilitas teknologi informasi lainnya. Setelah dilakukannya pencegahan, maka langkah selanjutnya adalah menetapkan hukuman terhadap tindak kejahatan yang mungkin terjadi. Hukuman harus berlaku secara professional dan tidak pandang bulu, baik untuk atasan maupun bawahan. Dengan mengetahui adanya hukuman, maka pekerja pun akan berpikir dua kali jika terbesit niat untuk melakukan sebuah kejahatan walaupun dia punya peluang untuk itu [4].

3.2. Aspek Lingkungan

Setelah mempertimbangkan aspek pekerja serta motif-motif kejahatan yang mungkin terjadi, langkah selanjutnya adalah memperhatikan lingkungan fisik institusi. Idealnya, sebuah lingkungan harus didesain untuk dapat meminimalisir terjadinya tindak kejahatan. Hal inilah yang selalu menjadi titik berat CPTED dalam mengantisipasi segala tindak kriminal yang mungkin terjadi, baik secara eksterior maupun interior.

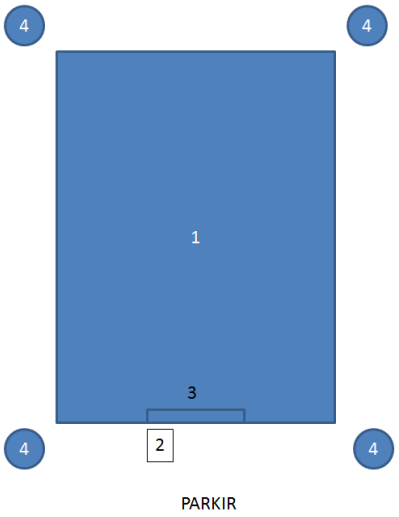
3.2.1. Ekterior

Desain ekterior sebuah bangunan merupakan garis depan dalam menghadapi ancaman dari pihak luar. Jika didesain dengan baik, maka para penjahat pun akan berpikir dua kali untuk melakukannya. Walaupun dalam kenyataannya, mendesain ulang keseluruhan eksterior untuk menciptakan lingkungan yang aman merupakan hal yang hampir tak mungkin dilakukan. Tapi setidaknya ruang-ruang yang ada tidak memberikan peluang untuk terjadinya tindak kejahatan. Menurut Atlas [3], desain ekterior yang baik harus mempertimbangkan empat hal utama yaitu kerapatan bangunan, pengawasan pasif, definisi ruang dan pencahayaan. Ke-empat hal ini tidak dapat berdiri sendiri karena merupakan suatu kesatuan unit yang tak terpisah.

Dalam CPTED ada tiga jenis ruang yang harus didefinisikan, yaitu publik, semipribadi, dan pribadi [2]. Ruang publik adalah ruang yang terbuka untuk semua orang dan tentu saja memiliki tingkat keamanan yang paling rendah [2]. Ruang semipribadi adalah ruang yang aksesnya hanya untuk sekelompok kecil orang [2]. Karena hanya sedikit yang mempunyai akses ke ruang ini, maka pengawasan pun akan lebih mudah dan efektif. Sedangkan ruang pribadi adalah ruang yang hak aksesnya sangat terbatas untuk orang-orang tertentu [2]. Ruang semi-pribadi adalah ruang perantara antara ruang publik dan ruang pribadi. Idealnya, setiap ada transisi dari satu jenis ruangan ke ruangan yang lain, harus ada ciri yang menunjukkan hal tersebut. Ciri ini dapat dalam bentuk penghalang secara fisik atau pun simbol. Contoh penghalang fisik adalah pintu, kaca, pagar dan penghalang lainnya yang dapat menghambat pergerakan secara fisik. Penghalang dalam bentuk simbol adalah salah satu bentuk pendefinisian ruang tanpa menghambat pergerakan secara fisik. Contohnya adalah pagar hiasan, garis di lantai atau pun perbedaan warna lantai.

Dalam hal pengawasan, ternyata ada yang terjadi secara alami. Pengawasan seperti ini masuk kategori pengawasan pasif. Seseorang yang selalu berada di suatu tempat secara terus-menerus akan secara pasif menjadi pengawas di lingkungan sekitarnya. Efektivitas pengawasan ini sangat bergantung dari banyaknya penghalang pandangan secara langsung. Makin luas jangkauan pandang seseorang, maka luas pula area pengawasannya. Untuk itu sangat perlu mengobservasi keseluruhan bangunan dari segala sudut pandang dan menentukan tempat yang tepat untuk dijadikan titik pengawasan secara pasif.

Kegelapan merupakan salah satu penghambat pengawasan pasif [1]. Solusinya adalah dengan memasang pencahayaan yang cukup. Ada beberapa hal yang harus diperhatikan dalam pencahayaan. Yang pertama adalah penempatannya dan yang kedua adalah intesitas cahayanya. Tingkat pencahayaan pada setiap area akan berbeda, tergantung dari tingkat kerawanan sebuah area terhadap tindak kejahatan. Semakin rawan suatu area, maka pencahayaan di area tersebut seharusnya semakin intens [1]. Hal ini dimaksudkan untuk menunjukkan kepada orang yang ingin berniat jahat bahwa area tersebut telah diawasi. Selain itu, jika dilakukan dengan benar, pencahayaan juga berfungsi untuk mendefinisikan ruang menjadi lebih jelas. Cahaya yang diarahkan ke suatu area dapat menjadi penanda bahwa area tersebut merupakan sebuah ruang tertentu.



Gambar 1. Usulan Desain Keamanan Ekterior

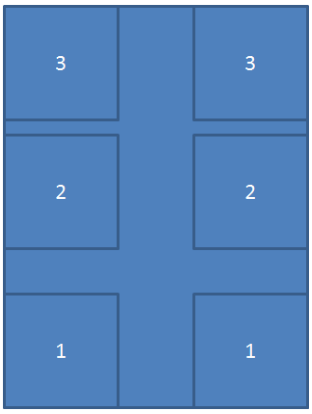
Keterangan:
1. Gedung utama
2. Penjaga pintu utama
3. Pintu masuk utama
4. Pencahayaan dan CCTV

3.2.1. Interior

Dalam CPTED, desain interior juga memiliki peran penting dalam meminimalisir tindak kejahatan. Hal-hal yang perlu diperhatikan dalam mendesain interior adalah garis pandang, pengawasan pasif, definisi ruang, dan karakteristik dari lingkungan interior itu sendiri. Ruang interior membutuhkan perhatian yang lebih karena di sinilah tujuan utama desain keamanan interior dan menjadi lebih kompleks lagi jika sudah berbenturan dengan desain fungsionalitas ruang [1].

Analisis terhadap aset institusi yang paling penting akan membawa kita kepada perencanaan keamanan yang efektif. Walaupun tidak mungkin menciptakan lingkungan yang 100% aman, tapi dengan adanya target aset yang ingin dilindungi, maka setiap perencanaan dan kebijakan yang dibuat akan selalu mempunyai tujuan yang jelas. Jika sudah teridentifikasi aset institusi yang paling bernilai, maka kita akan dengan mudah untuk fokus terhadap tindakan pengamanannya [3]. Dalam hal ini adalah tempat aset itu disimpan dan siapa yang akan diberi tanggung jawab terhadap ruangan tersebut.

Penentuan ruangan dapat dilakukan dengan menggunakan pembatas tertentu. Dinding, pintu, meja, serta tanda-tanda di lantai dapat dijadikan sebagai pembatas. Akses terhadap ruang-ruang tersebut dapat dianalogikan seperti lapisan-lapisan kulit bawang. Pergerakan individu harus dimulai dari ruang publik, ruang semi-pribadi dan baru ke ruang pribadi. Akses masuk harus dirancang sedemikian rupa, sehingga tidak ada akses langsung dari ruang publik ke ruang pribadi.



Gambar 2. Usulan Desain Keamanan Interior

Keterangan:
1. Ruang publik
2. Ruang semi-pribadi
3. Ruang pribadi

3.3. Standarisasi Infrastruktur

Setelah semua kebijakan tentang keamanan fisik selesai dibuat, tahap selanjutnya adalah upaya untuk menstandarkan semua infrastruktur yang ada. Mulai dari lokasi, ukuran, beban lantai, dinding, pintu, jendela, suhu, bahkan sampai sirkulasi udara sudah ada standarnya. Standar yang biasa digunakan untuk infrastruktur teknologi informasi adalah TIA-942 yang dikeluarkan oleh Telecommunications Industry Association [5] serta Information Technology Infrastucture Library (ITIL) [6]. Untuk institusi yang bergelut di bidang teknologi informasi, ruang komputer/ruang server merupakan aset institusi yang paling berharga [7]. Berikut adalah pembahasan mendetail mengenai standarisasi yang diusulkan untuk ruang komputer/ruang server berdasarkan TIA-942 dan ITIL.

A. Akses

Pintu ruang komputer harus dirancang untuk dapat diakses oleh orang-orang tertentu saja. Pengamanan tambahan sangat mutlak diperlukan. Dapat menggunakan penjaga khusus atau dengan alat tambahan biometric seperti pembaca sidik jari dan pemindai retina.

B. Ukuran

Ukuran ruang komputer harus memenuhi persyaratan penggunaan ruang untuk peralatan yang biasa digunakan, termasuk jarak antar peralatan tersebut. Sebagai contoh, misalnya sebuah ruang komputer akan dipakai untuk menyimpan 10 buah komputer. Setiap komputer memerlukan ruang 1m2. Jika jarak aman adalah 0.5m, maka ukuran minimal ruangan adalah 10 x 1.5m2 = 15m2. Ukuran lebih detail tentang peralatan-peralatan yang akan digunakan dapat kita tanyakan pada pemasok alat-alat tersebut. Sehingga perencanaan ukuran ruangan dapat dilakukan secara maksimal.

C. Peralatan Penunjang

Peralatan penunjang seperti pendingin udara dan UPS kurang dari 100 kVA masih aman untuk diletakkan dalam ruangan. UPS yang lebih dari 100 kVA harus diletakkan di ruang terpisah. Peralatan pendukung lain yang tidak berhubungan dengan ruang komputer tidak boleh dipasang di dalam ataupun melewati ruang komputer.

D. Ketinggian Langit-langit

Ketinggian minimum ruang komputer harus 2.6m (8.5 kaki) dari lantai terhadap objek yang tergantung di langit-langit seperti lampu, kamera dan lain-lain. Jika ada peralatan lain yang ukuran tingginya melebihi 2m, maka tinggi ruangan pun harus lebih tinggi lagi.

E. Pencahayaan

Pencahayaan minimal untuk bidang horisontal adalah 500 lux dan untuk bidang vertikal adalah 200 lux. Sumber listrik untuk pencahayaan tidak boleh sama dengan sumber listrik untuk peralatan utama ruang komputer. Sumber pencahayaan darurat juga harus disiapkan guna memudahkan pekerja menemukan pintu keluar saat terjadi musibah tertentu.

F. Pintu

Ukuran minimal pintu adalah lebar 1m dan tinggi 2.13m. Engsel pintu harus berada di dalam agar pintu tidak mudah dibuka atau dipindahkan. Pintu juga harus dilengkapi dengan kunci yang berkualitas. Pintu harus dirancang agar tidak mengganggu pemindahan alat-alat yang berukuran besar.

G. Beban Lantai

Lantai ruang komputer harus mampu menahan beban secara maksimal, baik beban yang terdistribusi maupun beban yang terkonsentrasi. Kapasitas minimal untuk beban yang terdistribusi adalah 7.2 kPA (150 lbf/ft2). Sedangkan yang direkomendasikan adalah 12 kPA (250 lbf/ft2). Lantai juga harus kuat menahan beban yang digantungkan pada lantai di bawahnya. Kapasitas minimalnya adalah 1.2 kPA (25 lbf/ft2), direkomendasikan 2.4 lbf/ft2).

H. Sirkulasi Udara

Dalam TIA-942 hal ini lebih dikenal dengan istilah sistem HVAC (Heating, Ventilation and Air Conditioning). Idealnya, sebuah ruang komputer memiliki sistem HVAC sendiri. Tapi jika tidak, lokasi ruang komputer harus terhubung langsung dengan sistem HVAC utama. Sistem HVAC ini harus handal dan mampu beroperasi 24 jam per hari, 365 hari per tahun.

I. Suhu dan Kelembaban

Untuk operasoinal yang terus-menerus, suhu dan kelembaban harus selalu dipantau dan dikendalikan. Berikut adalah panduannya.

- Suhu kering: 20º C (68º F) s/d 25º C (77º F).
- Kelembaban relatif: 40% s/d 55%.
- Titik embun maksimum: 21º C (69.8º F).
- Tingkat perubahan maksimum: 5º C (9º F).

J. Sumber Listrik

Sumber listrik untuk ruang komputer harus memiliki panel yang terpisah dengan ruang lainnya. Hal ini dilakukan guna mencegah terjadinya kelebihan beban listrik pada sebuah panel tertentu. Selain itu, jika panel yang lain bermasalah, panel ruang komputer tidak akan mengalami hal yang sama. Idealnya, ruang komputer juga harus memiliki standby generator yang terpisah. Jika tidak, panel ruang komputer harus terhubung langsung dengan standby generator utama institusi.

K. Pencegah Kebakaran

Ruang komputer mutlak membutuhkan sistem pencegah kebakaran. Sistem ini dapat berupa alarm kebakaran, alat pemadam api, serta sistem pemancar air. Semua peralatan untuk sistem pencegah kebakaran ini harus sesuai dengan standar NFPA-75.

L. Infiltrasi Air

Sistem drainase diperlukan jika terdapat risiko masuknya air ke dalam ruang komputer. Diperlukan minimal sebuah drainase untuk area seluas 100m2. Semua drainase dan pipa-pipa pembuangan air yang ada dalam ruang komputer harus berada jauh dan tidak tepat di bawah peralatan komputer yang ada.

4. Simpulan

Patut digarisbawahi bahwa CPTED hanya salah satu aspek dalam keamanan fisik. Perencanaan keamanan fisik yang efektif melibatkan banyak aspek seperti faktor finansial dan kelayakan fisik bangunan. Sangat tidak disarankan hanya bergantung pada CPTED untuk mengamankan fasilitas fisik. Sebagai batasan minimum, semua perencanaan keamanan fisik harus menggabungkan antara penggunaan bahan yang berkualitas, penempatan pekerja secara cerdas, audit dan invetarisasi secara berkala serta pemasangan perangkat pengaman tambahan seperti CCTV dan alarm.

Keputusan untuk meningkatkan keamanan secara fisik akan membutuhkan biaya yang tidak sedikit. Harus diperhitungkan secara matang untuk kepentingan jangka panjang. Jika kita menghitung jumlah kerugian akibat terjadinya pencurian dan pengrusakan, mungkin besarnya tidak akan sebesar biaya yang dibutuhkan untuk melakukan renovasi. Tapi jika kita pertimbangkan lagi untuk kepentingan jangka panjang, maka keputusan tersebut memang sangat layak untuk didukung secara finansial.

Daftar Pustaka

[1] R. Samuels. Afterdark Design, Night Animation & Interpersonal Interaction: Towards a Community-Security Paradigm. *Journal of Architectural and Planning Research*. 2005.

[2] G.R. Cook. CPTED Makes a Comeback. Crime Wise Library. 2003.

[3] R. Atlas. The Other Side of CPTED. Crime Wise Library. 2001.

[4] J.A. Walsh. Employee Theft. International Foundation for Protection Officers. 2000.

[5] TIA-942. *TIA Standard*. Telecommunication Industry Association. 2005.

[6] S.M. Ali, T.R. Soomro. Integration of Information Security Essential Controls into Information Technology Infrastructure Library. *IJASTNET*. 2014; Vol 4.

[7] H. Hamidovic. Fire Protection of Computer Rooms - Legal Obligations and Best Practices. *ISACA Journal*. 2014; Vol 4.