Global Information Assurance Certification Paper

Using Passive Environmental Cues to Enhance Physical Security

By David R. Pollack

Submitted as part of SANS GSEC Certification
Assignment 1.4b
6 May 2004

Introduction

Strong passwords, intrusion detection systems, properly configured firewalls and routers, up to date anti virus software, properly patched operating systems, solid backup schemes and qualified security personnel are some of the most important aspects of information security. All of these things help safeguard data from the potentially devastating effects of a determined hacker because they make unauthorized access to your network harder to attain.

Unfortunately, this threat is not limited to the electronic medium. Most computer users are not aware of the fact that malevolent individuals use a variety of methods to gain access to systems including social engineering and outright theft. All too often do people rely on electronic security devices to provide all of their information security needs. An electronic device such as an IDS may detect someone attacking a web server, but it will not detect someone at a terminal stealing data or equipment.

If a person has physical access to a workstation or server, they control that system and the data stored on it. This is an important fact to consider because it highlights the idea that sound electronic security is only part of the security game. Physical security is the other. It is what enables all other security measures to perform effectively and it is an absolute necessity in any comprehensive security plan.

Summary

Physical security is an extremely broad topic. It encompasses access control devices such as smart cards, air filtration and fireproofing. It is also heavily reliant on infrastructure. This means that many of the ideal physical security measures may not be economically or physically feasible for existing sites. Many businesses don't have the option of building their own facility from the ground up thus physical security often must be integrated into an existing structure. This limits the overall set of security measures that can be installed.

There is an aspect of physical security that is often overlooked; the humans that interact with it. Humans commit crime for a number of reasons. In considering a plan for improved physical security, it is important to consider the motives and situations that facilitate the committing of crimes in the workplace. After all, the very employees that are entrusted to perform security and support functions may be the individuals committing the crimes.

This paper is an exploration of some alternate physical security measures. The methods and ideas conveyed in this guide are passive in nature and are based on the ideas of CPTED. CPTED is an acronym for Crime Prevention Through Environmental Design.

> "The basic concept of CPTED is that the physical environment can be changed to impact criminal behavior in a way that will reduce the incidence and fear of crime and improve the quality of life."(Cook)

CPTED focuses on four areas to achieve this goal:

- Access control
- Surveillance
- Activity support
- Motivation reinforcement.

Many security professionals rely too heavily on active security measures such as alarms, guards, locks, card readers, and CCTV. While one cannot refute the effectiveness of all of these methods, more attention should be focused on the *causes* of criminal behavior in the workplace and how the environment can take advantage of the crime-security relationship. If an office is organized in such a way as to contradict criminal behavior, the net outcome will be improved security.

The Employee Aspect

Security threats originate from internal and external sources. Internal sources are employees. External threats are everyone else including former employees. Employees should be the biggest concern in every security plan. The reason for this is twofold. First, employees are in the position to cause the most harm. Secondly, 85% of theft and fraud in US industries originates from employees. (Bell) If employees are hired to support a business, why would they turn around and bite the hand that feeds them? Employees steal from their employers for a number of reasons and understanding these reasons will give a more comprehensive understanding of how to tailor a security plan to the business' specific needs.

- Low morale in the workplace (Walsh) – Employees may be motivated to steal from their employer if they feel they have no way of moving up the corporate ladder. Their rationalization for theft is that they aren't going anywhere in the company anyway.

- Employee feels wronged by employer (Walsh)– Often if an employee was punished unfairly they may seek revenge in the form of abusing their access or privileges to hurt the entity that has caused them pain.

- Employee feels under compensated (Walsh)– Employees have their own notion of what their labor is worth. If an employee feels that their wages or benefits are far below their notion of their own value to the business, they might steal to make up for the deficit.

- The consequences of the theft are minimal (Walsh)– Employees may feel that stealing from their employer is not a really significant. There are a few scenarios that can cause this behavior. One may be that an employee takes notice of a co-worker who was caught stealing and his punishment wasn't severe. Another aspect is the gross revenue of the company itself. Employees may feel that stealing a $75 USB memory stick is nothing to a company that brings in $50 million dollars of business per year.

- Debt and expenses (McKaig)– If an employee salary is insufficient to cover personal expenses, an employee may steal merely to survive economically.

- Espionage – Employees may be hired by competitors to divulge information or steal sensitive equipment and data.

- Opportunity – Many employees steal for no other reason than opportunity. Even employees who have never stolen before may find themselves doing so if they know that no one will catch them. Opportunity is the leading cause of theft in all businesses. (Walsh) Lack of surveillance, inventory control, and anti-theft devices offer employees a highly tempting situation.

Now that the most common motives for theft are clear, attacking them is a good way to reduce theft. One of the best ways to stop criminal behavior in the workplace is to not hire criminals. Human resources should thoroughly screen every potential employee. Resume information should be verified and criminal background checks should be done. (Terrill) This is especially important if the applicant is someone who will be assuming an information or financial sensitive position.

In addition to background checks and resume verification, interviewers should discuss theft and loss prevention at hiring. Policies regarding theft, misuse of company assets, and other inappropriate workplace behavior must be clearly stated and punishments for this behavior clearly laid out. (Terrill) This establishes ahead of time an understanding with the applicant that theft is something the company is aware of and takes seriously. This effectively eliminates motives relating to mild consequences and undermines motives stemming from employees who feel they were unfairly punished. Knowing the consequences of theft ahead of time will make it harder for employees to rationalize feelings of being wronged. It is also important to consider that the same professional behavior that is expected of lower level employees should be expected of upper level executives. (Terrill) If a lower level employee sees his boss steal from the company without repercussion, he too will think it is alright to do the same. If the lower level employee then gets caught and punished, the company might be creating criminal motives in the employee.

Debt and expenses motives can be stopped if the employee has a way to seek help from within the company. Businesses that have the ability to assist their employees with financial problems will have much lower instances of theft as a result of debt motives. Programs such as debt restructuring, company loans or pay advances attack this theft motive from two angles. First they help eliminate the initial cause of the motive and they foster a feeling of gratitude and affinity to the company.

Low morale and feelings of being underpaid are difficult to counter for a number of reasons. Morale is not something that is very tangible or easily measured, but very important nonetheless. Wages are also difficult not because it is intangible like morale, but it is hard for a business to increase salaries because one of their employees feels they deserve more. A solution to these problems is the concept of company culture.

The idea of a company culture is that the employees of a company develop a sense of belonging and importance within their organization. With this comes a greater feeling of ownership and solidarity. It also tends to shift the employee's idea of worth in the business from the amount on their paycheck to the positive contribution their position makes to the company. Increasing communication between employees develops corporate culture. Regular meetings about important corporate issues such as theft and shrinkage make employees feel they can take part in corporate decisions. (Terrill) This will often result in an increased feeling of corporate ownership among employees.

Reducing the window of opportunity someone has to steal is the single most effective way to reduce theft. Opportunity motives can be reduced by effective surveillance, inventory control, and frequent detailed audits. In addition, employees must be aware of these anti-theft measures because that is what actually minimizes the perceived opportunities to steal. In addition to the frequency, the audits should be performed in a randomized manner. If there is a weekly audit of equipment, employees know when equipment or inventory is most vulnerable.

There are a few other important things that can have a positive effect on theft in the workplace. Education about criminal behavior and theft among employees and managers is important because employees often do not realize they are stealing. (Terrill) For example, an employee decides to make a long distance call to his mother during business hours on a company cell phone. While this seems harmless enough, it may be considered theft because the employee is getting paid for time he is not working, and he is charging a phone call to his company that is not business related.

In addition to education, it is important to consider is the procedure for reporting criminal activity. While it may be easy for an employee to report crime committed by an outsider against the company, it may be difficult to report theft within the company out of concern for job and reputation. Businesses should consider creating anonymous hot lines where employees can report criminal behavior without revealing their identity. (Terrill) Care should be taken in following up anonymous tips however, because it is not a good idea to wrongly accuse and alienate employees. This could cause a situation where an employee feels wronged and may wish to retaliate.

The Environment and Crime

After careful consideration of employees and their motives for crime in the workplace, an examination of the physical environment of the workplace is next. Ideally, the environment should be designed to discourage criminal behavior by making it either harder to commit a crime or harder to commit a crime unnoticed. These are the environmental pressures that the four goals of CPTED try to place on potential criminals. In reality, it may not be possible to redesign the entire exterior of a building to create these environmental cues, but at a minimum, spaces should not provide support for criminal activities.

The exterior design of a building is the first line of defense against external

threats. If designed well, most criminals won't look twice at the building because they will feel it is too risky to partake in criminal behavior at the site. To achieve this result, there are four major areas to consider in the design of a building's exterior; adjacent properties, surveillance, definition of spaces, and lighting. These four areas do not work independent of one another and therefore it is important that they all be considered together as a security unit rather than separate measures.

Consideration of adjacent properties is important because it forms the foundation of the exterior design of a secure facility. Some businesses attract more crime than others. For example, clubs, bars and public transportation facilities are areas of high crime victimization. (Wood) These areas have the highest instances of violent attacks, employee theft, and vandalism. (Wood) Other high-risk areas include gas stations, bars and clubs. (Wood) Since these areas attract a high volume of potentially dangerous individuals, exterior planning should consider these areas as the main sources of crime and thus seek to shield the premises from these sources.

Clearly defining space as belonging to someone is in itself a crime deterrent because it makes it easier to spot individuals who occupy the space. (Atlas) If an individual can be easily spotted in a defined area, that individual will be less likely to commit a crime in that area because the risk of being caught is elevated. CPTED points out that there are three classifications for spaces; public, semi-private, and private. Public space is open to all and it is the least secure. There is little or no opportunity for extensive surveillance. (Gardner) Semi-private spaces are areas that have some means of restricting access and thus are only open to a smaller group of people. Because there are less people within this space, surveillance of these spaces is more effective. Private spaces are areas where access is further restricted to a smaller select group of people. A semi-private space is used as a buffer between public and private spaces. Ideally, any time there is a transition from one type of space to another, there should be some environmental cue that signifies this transition. (Gardner) This cue can be in the form of a physical or symbolic barrier. Physical barriers are doors, glass, fences or any other physical object that prevents or alters physical movement. A symbolic barrier is one that defines a space without actually preventing physical movement. Examples of this are low decorative fences, signs, or even changes in sidewalk materials. (Gardner)

Natural surveillance is surveillance at a passive level. Individuals who are suppose to be in the area constantly and passively monitor their surroundings. (Cook) The effectiveness of such surveillance is influenced directly by the number of obstructions in the sight lines at the facility. (Gardner) Trees, shrubs, fences, buildings, and cars are the kind of objects that can negatively impact natural surveillance. It is important to observe a facility from multiple angles and prioritize natural surveillance points. For example, is the entire parking lot visible from the entrance of the building? This helps employees spot a potential assailant waiting in the parking lot and thus gives the employee the opportunity to avoid them. In addition, good sight lines will deter assailants from victimizing individuals at that facility because they cannot surprise their victims and are more at risk of being seen.

Darkness diminishes the level of natural surveillance. It is therefore necessary to install lighting to counter this problem. There are a few things that must be considered with lighting. First is placement of lighting fixtures. The other is the intensity of the light emanating from the fixtures. At a given facility, there will be areas that are more vulnerable to criminal activity. Lighting placed in this area should be more intense than less vulnerable areas. (Gardner) This conveys the idea to the potential perpetrator that this area has more attention focused on it therefore removing much of the weakness inherent in the area. In addition, lighting serves to accentuate the definition of space if used properly. (Gardner) A light beam directed at an area has definite borders that can be used to create an environmental cue that the type of space has changed.

An example of a CPTED-friendly exterior design is shown in figures 1 and 1a. This particular site has two crime sources in the form of a public train station to its north and a strip of bars and clubs to its east. In order to cope with these crime sources, the designer employs a combination of small decorative hills densely planted with tall bushes that extend the entire length of the northern and eastern property lines. This serves two purposes. First it breaks any sight lines from the crime sources to the site. If an individual can't see a target, they will probably be ignorant of its existence. Secondly, the hills and trees clearly define the property lines of the site and makes spotting an individual on the property easier. There is also a line of low shrubs along the western and southern property lines. The designer chose to define the parking lots and entrance to the site as semi-private spaces. The sidewalk and street in front are public zones. Despite the fact that the driveway breaks the line of shrubs along the southern property line, the overall feeling is that by crossing this line one is entering a controlled area. This is a passive form of access control.

The level of natural surveillance of this site is superb. Employees can clearly see the entire parking area and the entrance to the building simply by driving up to the site. In addition, law enforcement on their normal patrols can quickly spot anyone on the premises after hours. Leaving the site, the entrance is situated at the southeastern corner of the building. This allows unfettered sight lines from the entrance over the entire premises including the sidewalk and street. Any vehicles or individuals approaching the site are easily spotted from most points in the parking area especially from the entrance of the site. Simply based on the high level of natural surveillance in this design, the exterior provides little or no support for criminal activities because the chance of being observed is too great.

There is one very important aspect to consider regarding sight lines, surveillance and landscaping. Prior to planting any form of shrubbery, trees, or flowers, the growth characteristics of the plants must be taken into account. (Gardner) In this example, if the shrubs and bushes planted along the southern have an aggressive vertical growth tendencies, they will require frequent trimming to maintain good sight lines and natural surveillance. This is especially important in high vulnerability areas where visibility is already limited and the potential for crime high.

Exterior lighting at this site is used to maintain the high level of natural

surveillance and to further augment spatial definition. Lights are placed at the northeast, southeast, and southwestern corners of the property. These lights are elevated considerably to increase their effective lighting range. An important fact about these lights though is that they have shields to prevent their light spilling over onto neighboring properties. Figure 1a shows the light beams on the east and west edges of the property ending at or near the property lines. At night, this further accentuates boundaries to define where the site starts and ends. There are three more lights in this example. One is placed on the southern face of the building while the remaining two are placed on the eastern face. These lights help illuminate the parts of the parking lot that the three post lights might not effectively reach.

The intensity of the lighting on this site varies across the different areas. The northern most lights are the brightest because they light the area furthest away from the entrance to the building and the road. This is the most vulnerable area because it is the furthest from the road and has some mildly obstructed sight lines from certain viewpoints. The brighter lighting in this area inhibits crime because it increases the possibility of being noticed while occupying this area.

In addition to preserving sight lines and natural surveillance, a well-lit site creates a bright and cheerful environment that has another important effect on potential criminals. It gives the impression that the site and all its occupants are a cohesive unit that are conscience of their surroundings and have taken extra care in planning and organizing the property. This is a crime deterrent itself because it suggests that there is a significant attention to detail and spatial ownership, where an outsider will be easily recognized on the premises. (Cook)

Inside

The same CPTED principles that apply to exterior design apply to interior spaces as well. Consideration of sight lines, natural surveillance, definition of spaces, and the characteristics of the interior environment all play key roles in the design of a secure facility. Interior spaces require extra attention though because this is the area all security measures aim to protect, and the design pressures of spatial functionality become more complicated. A building with four concrete walls that are five feet thick with no doors and windows is very secure, but not very useful. Security measures therefore must coexist with the necessity to allow easy access and use of the space while preventing theft and other criminal activities from taking place.

Just as the adjacent properties of a site should be considered when designing a security plan, the interior characteristics of the building should be examined thoroughly. All points of entry to the building such as doors, windows, skylights, storm sewers, roofs, floors and fire escapes should undergo scrutiny. (Atlas) Doors and windows offer the greatest vulnerability due to the inherent ease of access to them. (Atlas) When looking at these points of entry, the building materials that windows and doors are constructed of should also be looked at. In addition, it is a good idea to use mantraps at the entrances to allow employees to screen individuals prior to entering the work area. (Cole) A server

room locked within a sheet rock walled room is easy to gain access to with a hammer. Likewise, a hollow wood door can be kicked in with one stiff blow. (Atlas) The construction of walls, doors, hinges and windows must be adequate to the extent that they can effectively control access to the spaces they separate.

The location of existing storage areas, server rooms, supply closets and manager offices must be considered as well. Depending on the type of business, certain areas may be inherently more vulnerable to theft and damage by employees or outsiders. In a business that keeps an inventory of goods or has a lot of small and easy to steal equipment, storage rooms might be the highest vulnerability areas. In a business where data is the most valuable asset, server rooms or filing areas might be the most vulnerable. This brings up an important aspect of any effective security plan. Often it will not be possible to create a perfectly secure environment. As a result, all security policies and plans must have a target asset in mind. (Atlas) Once the most valuable asset(s) is identified, focused security measures can be put in place more easily. In this situation, identifying which areas are most vulnerable or mission critical will influence the placement and orientation of employee work areas.

Utilities are another issue. Where do they come into the building and who has access to them? Damaging or disconnecting utilities is an easy way to bring a business to a grinding halt or to defeat some active security measures such as CCTV or alarm systems (Atlas). All utilities should be protected and access restricted only to those who need access to them. (Atlas) If the utility boxes (fuse panels, relays, telephone circuitry) cannot or are not isolated in a closet or room, simply placing locks on the boxes or replacing the boxes with ones that can be locked can go a long way in protecting them.

Once a careful analysis of the building infrastructure is complete, weaknesses mitigated to a satisfactory degree, and valuables identified, desk design, placement, and orientation is the next consideration. The overall idea in protecting a sensitive area is to increase the level of natural surveillance in the area. (Cook) If there are ten employees located near and facing a server room door, an individual entering or leaving the room will likely draw attention. Floor plans for employee desk positions should therefore take advantage of this idea. Entrances and exits should also be considered vulnerabilities and as such, should have employees or guards watching them. If possible, the employee or guard watching the area should have the ability to deny access to someone trying to enter the premises either through the use of a mantrap or a self locking door that requires someone from the inside to open it. (Cole) The most important thing though about this is that the employees have the chance to evaluate the individual wishing to gain admittance prior to the individual entering the premises. (Cole) Employee desks should not be so tall as to prevent employees from effectively scanning the area in around their desk. This also allows management to scan the office and see which employees are at their desks.

The placement of employee work areas cannot follow this principle blindly however because guest circulation and access is another issue that must be considered when planning the layout of the office. Definition of space can be used to provide

environmental cues to help prevent guests from wandering into areas where they should not be. It can also help employees identify outsiders in sensitive areas. The first step is to determine what types of areas are needed in the office. If the business needs to be able to accommodate guests, then there will be the need for public spaces. If guests are not usually anticipated, then all of the space inside the office will be semi-private and private. Dividing and defining these spaces can be done in a number of different ways. Desks, walls and doors can be used to form physical barriers while signs and changes in floor materials can be symbolic barriers. In any floor plan and space definition scheme, the idea is to layer access and security measures like an onion. (Atlas) Movement of an individual should go from public to semi-private and finally to private space. There should not be a way to go directly from public to private spaces.

Business should also consider allowing employees to personalize their work areas within reason. This form of motivation reinforcement can foster a feeling of territoriality because it allows the employee to define their area as exclusive to themselves and take control of it. (Gardner) An employee will be much more sensitive to intruders if there are valuables of the employee in their workspace. Employees should not be allowed to break sight lines with personal items like plants. This can negatively impact natural surveillance of the interior space.

Figure 2 is an example of an office layout that incorporates the passive security measures discussed above. There are two doors into and out of the premises; one main and the other an alarmed emergency exit. Both of these exits are relatively far from sensitive storage and utility areas. In addition, the utility closet can be locked and it is separate from the storage and supply rooms. This makes the storage areas less vulnerable because individuals who need access to the utility closet do not have to be in the storage area and it prevents individuals without a key from tampering with utilities.

In addition, the main entrance area serves as a large mantrap that allows the guard or secretary at the front desk to greet and assess visitors and employees easily. There are two doors that exit the mantrap. Both of these doors have electronic locks that the guard or secretary must disengage to allow the individual into the semi-private and private areas of the office. These doors serve as the first transitional cue from public space to semi-private spaces. After passing through either door, there is a low wall that serves as another demarcation of a defined space. In this case, it is the transition from semi-private to private space. There are breaks in the wall that allow entry into the private spaces, however at each entry is a sign that states “Authorized Personnel Only.” This serves as a symbolic barrier that will educate the unintentional intruder (Cole) and keep them from wandering into sensitive areas. On the opposite side of this wall are fully enclosed offices with windows facing the general work area. This layout limits the semi-private area only to the walkways themselves making it easy to spot someone within private spaces. The bathrooms are located away from sensitive areas so as to keep unnecessary traffic away from vulnerable areas. A secure design should not give an unauthorized individual a valid excuse for being in a sensitive area.

Workspace arrangement of this example layout heightens the level of natural

surveillance in the office. All desks and furniture are relatively low allowing unfettered sight lines across the entire office. There are lines of desks bordering each walkway. This makes it nearly impossible to sneak unnoticed to a private space. In addition, there are lines of desks in the back portion of the office facing the storage and utility rooms. This allows easy passive surveillance of an individual entering and leaving these areas. A utility worker trying to access a storage room will likely be noticed by the large number of employees facing that area. The offices that border the outside of the site have windows facing the work areas that allow the occupants of the office to monitor activities within the work area.

Common Sense Measures

It is important to keep in mind that CPTED is only one aspect of physical security and that an effective security plan incorporates as many measures as economically and physically feasible. It is *not* recommended in any way to rely on CPTED as a silver bullet solution. This paper has intentionally omitted an in-depth discussion of many basic security measures in favor of examining the topic of CPTED more thoroughly. At a bare minimum, all security plans should incorporate the use of quality locks, intelligent distribution of the keys for those locks, frequent but random audits of equipment and inventory and hardware anti-theft devices.

Conclusion

The decision to enhance the security of a given site is always accompanied by a budget for the enhancements. This budget is based on the perceived financial damages of losing a laptop, server, safe, client, or labor. It is vitally important that the perception of damages not be underestimated. In 2000, employee theft cost U.S. business over $50 billion. (Walsh) In addition, the same study found that 75% of all employees steal at least once throughout their careers. The theft of a single laptop costs U.S. business an average of $89,000 per incident, which is second only to damage caused by computer viruses. (Laptop Theft) With these figures in mind, is $150,000 for office renovation to improve security too much to protect the ten laptops in the office? While the national average may not be accurate for one particular business, the loss off equipment, data, or personnel will still be significant and therefore must be taken seriously.

FIGURE 1 (Drawing by David Pollack)

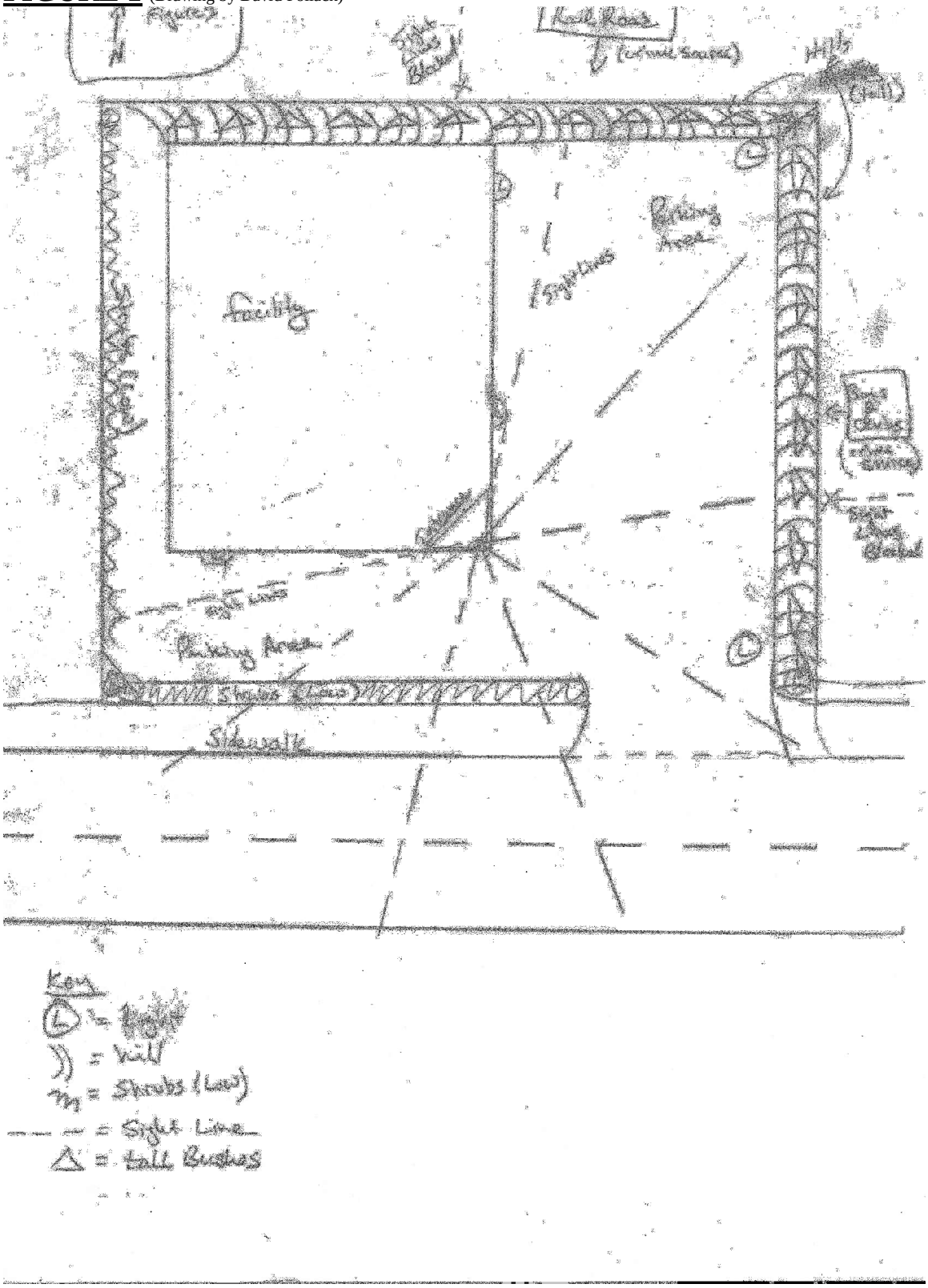


FIGURE 1a (Drawing by David Pollack)

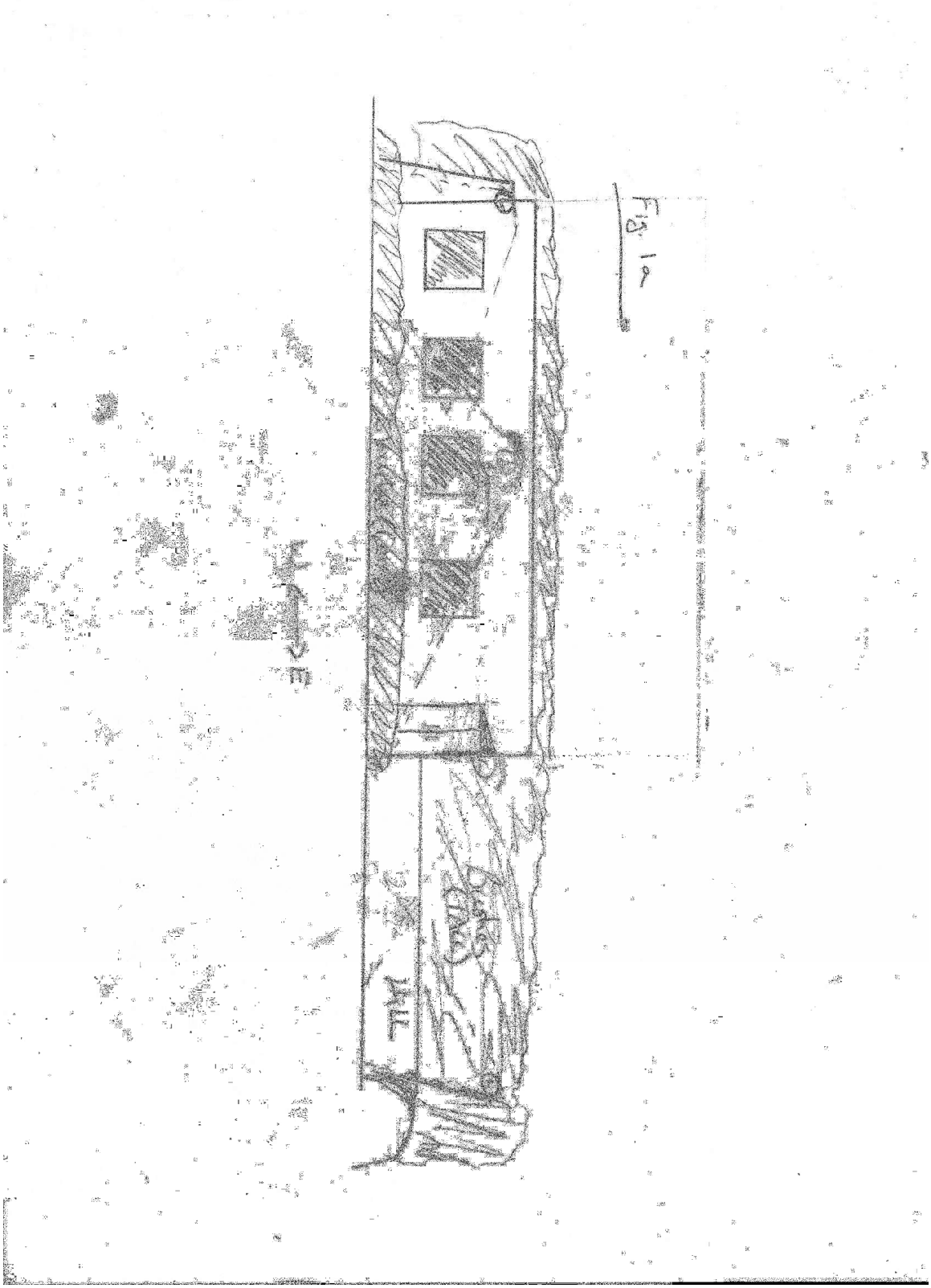
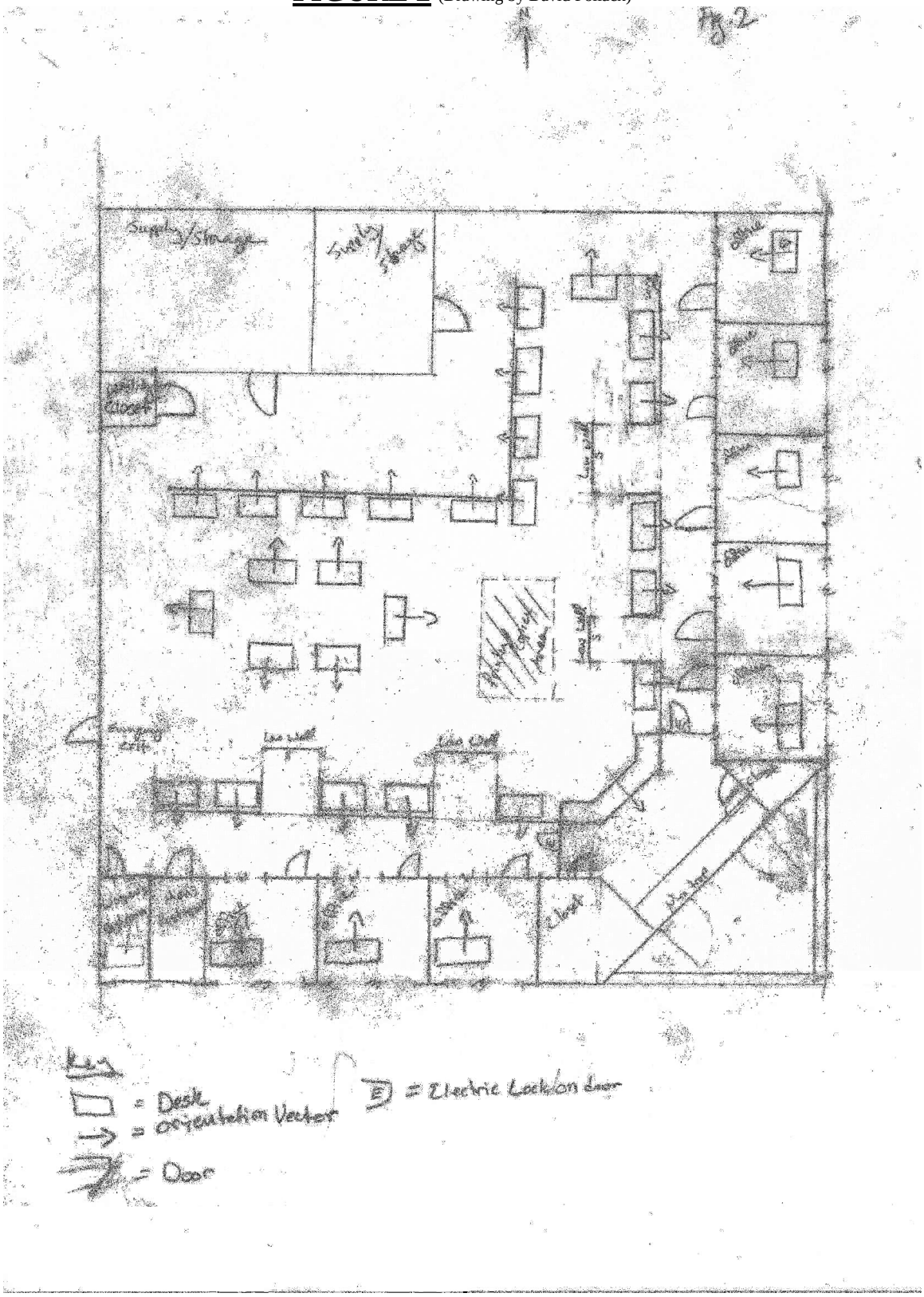


FIGURE 2 (Drawing by David Pollack)



References

1.Cook, Gary R. CPTED Makes a Comeback. <http://www.vcnet.com/expert/library/cpted_gc.html>.

2.McKaig, Ryan. Designing for Security Can Help Keep Intruders at Bay. 20 June 2003. <http://triangle.bizjournals.com/triangle/stories/2003/06/23/focus2.html>

3.Walsh, Justin. Employee Theft. August 2000. <http://www.ifpo.org/articlebank/employee_theft.htm>

4.Terrill, Kevin. Preventing Employee Theft – Training the Internal Watchdog. 9 June 2002. <http://www.bankersonline.com/security/internalwatchdog.html>

5.Ryder, Josh. Laptop Security Part I: Preventing Laptop Theft. 30 July 2001. <http://www.securityfocus.com/infocus/1186>

6.Atlas, Randal. Architect Input Among First Steps in Design. June 1991. <http://www.cpted-security.com/cpted1.htm>

7.Atlas, Randal. Building Design can Provide Defensible Space. September 1989. <http://www.cpted-security.com/cpted3.htm>

8.Cole, Eric, et al. SANS Security Essentials with CISSP CBK. SANS Institute 2003.

9.Bell, Arthur H. Guarding Against the Unthinkable... Employee Theft and Fraud. March 2003. <http://www.rentalmanagementmag.com/newsart.asp?ARTID=896>

10.Laptop Theft Statistics. 2002. <http://www.microsaver.com/html/2178.html#stats>

11.Gardner, Robert A. Crime Prevention Through Environmental Design. 1995. <http://www.vcnet.com/expert/library/cpted.html>

12.Wood, J, et. al. Crime Against Small Business: Facing The Challenge. 1997. <http://www.crimereduction.gov.uk/toolkits/br020302.htm>