DATA CENTER THREATS AND VULNERABILITIES

Jonathan A. Zdziarski
jonathan@zdziarski.com

Abstract

Data center facilities are at the heart of today's electronic infrastructure, giving life to a significant percentage of online commerce. Due to their planned construction on critical infrastructure, such as converging power grids and dense telecom networks, they are also, however largely unguarded potential targets for terrorists. Data centers are among the only facilities located globally within proximity to mission critical infrastructure, where even a lightly funded individual is clear to install heavy equipment virtually unchecked and undisturbed for long periods of time, with access to a remote high-QoS network (the Internet) as a detonator. Because private data centers are largely ubiquitous in their procedures, which typically do not include hardware inspection, this would allow a terrorist group to launch a national, distributed, coordinated attack taking out many large cities' infrastructures simultaneously, and without prior detection.

1. Introduction

Data center facilities are commonplace in today's vast telecommunications infrastructure as an inexpensive solution for high speed Internet access. These and other such hosting facilities provide cost effective connectivity for computer equipment in a remote, climate-controlled environment, usually with several redundant high-speed connections to the Internet. These facilities are responsible for a significant percentage of electronic business performed in the United States and other countries and provide hosting for organizations ranging from financial institutions to adult websites and spammers.

Prior to September 11, 2001, the notion of an attack using data center facilities seemed infeasible to most of the private sector, however this viewpoint has changed, and these facilities now appear as a logical target for terrorists, allowing a group to potentially launch a successful, distributed attack against surrounding critical infrastructure. Many data center facilities are strategically placed in areas where significant commerce is occurring in order to take advantage of the abundant infrastructure in the area. Along with these come major Internet exchanges (peering points), large corporate concentrations, and many possibly high-profile targets such as financial institutions, news buildings, and political targets. Some facilities are within immediate proximity to targets such as the New York Stock Exchange, the CNN building, and the public and private networks that are responsible for the Internet as well as military and public service networks. Due to the placement of such facilities, they are more than likely targets.

Data center facilities are among the only facilities located globally within proximity to mission critical infrastructure where even a lightly funded individual is able to install heavy equipment virtually unchecked and undisturbed for long periods of time with a remote, high quality of service (QoS) network. Too, this network can be synchronized to launch attacks involving multiple simultaneous targets can be coordinated from anywhere in the world or made to operate autonomously based on specific predetermined events, including for example:

- A daily news search for a specific event, and a match threshold
- The price of a certain share of stock
- Extended dark periods in reaching a specific Internet Protocol (IP) address
- Simple date and time of the machine

To summarize, data centers are an ideal target for terrorists to use because it provides all of the important ingredients for a distributed, coordinated attack:

- Easy introduction of concealed explosive devices, even a small nuclear device
- Presence in a large metropolitan area
- Presence of significant mission-critical infrastructure
- Remote access to detonate device(s)
- A planning period that can stretch months or years
- Opportunity for extraction prior to detonation

Such an attack in one single area would easily leave thousands without electricity, emergency services, and other such critical services. Historically, these conditions frequently lead to a significant loss of commerce, high rate of crime and possible loss of life.

2. Anatomy of a Data Center

Before exploring the different vulnerabilities these facilities are challenged with, it's necessary to have a general overview of what comprises the average facility.

2.1 Components

A data center is typically a large, spacious facility located either in a dedicated building (also referred to as a "server farm") or leased space within an office. Slices of space are leased to the data center's customers, who are responsible for moving their equipment into the facility, setting it up on racks or in cages, and connecting it to (usually backbone) networks provided by the facility. Most facilities are comprised of the following components:

- Telecommunications equipment for network connectivity
- Racks for mounting of customer equipment with overhead conduits for cables
- Cages or cabinets to physically isolate systems
- A raised floor for air conditioning, power, conduits, and flood prevention
- A fire control system (usually a Halon, Carbon Dioxide, or Potassium-based system) and crash-and-hold bars on all doors
- An authentication system for entrance and exit; this may include a card reader, biometric device, or manned security post.
- Security cameras to view an overall state of the facility

Most facilities are unmanned, and remotely managed from a network operations center (NOC). This NOC may be located in an adjacent room, on a different floor, or in a

nearby building. The NOC is usually responsible for the electrical and environmental state of the entire facility including its network, hosted equipment, and etcetera.

2.2 Access Procedures

Other than employees of the facility, there are typically two classes of individuals clear to access these facilities at various times:

1. Telco and equipment technicians, fire marshals, building personnel and other authorized technical or building staff.

2. Customers who have procured space

2.2.1 Maintenance

Maintenance personnel seeking access to the facility will generally be required to provide an identification card and/or information about the service call. Because the maintenance may be on behalf of a specific customer, an access ticket may be required to permit the individual into the customer's cage or cabinet. An individual performing maintenance on the facility may be from one of many local carriers with hardware in the facility, an electrician configuring a rack for a customer, fire marshal (who frequently inspect facilities), or a technician from a customer sent out to service a system. Guest cards are usually granted to the technician upon arrival, or the technician is escorted into the facility and left to work.

2.2.2 Customers

The standard procedure to procure rack space in a data center is to sign and pay on a contract (usually annual) through the company's sales representative. The customer's network access will then be provisioned and rack space assigned. Access control for customers is typically formal. The customer may be granted access cards, a key, or other means to access the facility at which point it will be their responsibility to install their equipment and bring it online. Biometrics may be in use as well to prevent access card theft.

Because a majority of data center facilities are unmanned (perhaps with the exception of a security guard), it is the customer or technician's responsibility to conduct themselves in a professional manner by not stealing or sabotaging the equipment of another customer or vendor. Frequently, this is left to physical security by means of caged equipment or locked cabinets. Should an individual visit the facility during a lull time (the evening, for example), one may be virtually alone. The individual will usually bring the necessary equipment in on a cart, swipe a card, possibly sign in, and be cleared for access to the facility. Due to confidentiality concerns, customers are typically not monitored unless there is a pressing need.

2.3 Presupposed Innocence

Security staff and procedures are in place to ensure that unauthorized individuals are not permitted into the facility – to discourage an individual from an overt attack such as walking in with a baseball bat and smashing equipment. Security staff is not by any means equipped with the ability to determine if a chassis is armed with explosives or sometimes even if the equipment a customer is working on belongs to them. The perception to staff working in a data center facility on a daily basis is typically limited to access only and not to equipment. Customers and their equipment is presupposed to be innocuous, even by engineers in the facility - and is therefore rarely ever challenged. Authorized guests of the facility will occasionally introduce large pieces of heavy equipment into the facility on behalf of a customer or telecommunications provider. These can include enterprise-class servers or mainframes, network or telecom equipment, large batteries, and possibly even customer-owned hardware closets. It is not uncommon to see computer systems five or six feet high with large locking doors for disk storage or processor blades nor is it uncommon to see a group of deep-cycle batteries with bare terminals connected to equipment. Other equipment involved usually includes copper and fiber optic cabling, miscellaneous small devices, and possibly even the customer's own remote access devices. All forms of this equipment are considered innocuous due to its necessity in the telecommunications space.

3. Reconnaissance: Research for an Attack

Before determining the right kind of attack, the attacker may launch a reconnaissance mission to collect intelligence about various weaknesses in the facility's procedures or to gather needed information, such as customer names. A facility's account executives are, like all other sales associates, usually eager to give a guided tour through their facility to a prospect and may drop names of larger customers. Company logos and machine hostnames/addresses are also likely to be visible. The walk through and covert interrogation of the account manager also gives a potential attacker:

- Names of some customers and possibly (via labels) IP addresses and hostnames of some of their equipment.
- A relationship with the sales representative, who may also introduce him to facility staff, establishing a level of familiarity.
- Location of most or all security cameras, if and how they are recorded, and the frame-rate and size of the capture.
- Understanding of the general security in the building, entry practices, hardware policies (if any), and etcetera.
- Knowledge of any businesses in the facility that would make good targets
- Knowledge of the part of the city they are located in and what targets are nearby, what power grids and telecommunications networks support the facility, etcetera
- How much space the attacker will have to place their equipment, and where
- Typical hours of operation, staff rotation, and other internal operational data

Once the attacker has this information, they can make an even better judgment about whether or not the facility is a suitable point of attack and select a method of insertion.

4. Exploiting Facility Weaknesses

In this section, we will discuss the various weaknesses in many data center policies and illustrate some possible scenarios of how a malicious group could possibly exploit them.

4.1 Maintenance Practices and Social Engineering

Telecom, fire, electrical, security, building management, and customer equipment vendors are just a few of the many different maintenance personnel frequenting a data center. Even well established procedures are vulnerable to social engineering, which requires only common knowledge of a related engineering field and manipulation skills to gain access to a data center. While it is unlikely that a terrorist will choose this type of attack over the second type of attack we will discuss (becoming an actual customer), we will briefly discuss this possibility and why the vulnerabilities exist.

Because many visits (particularly emergency visits) can go unannounced at the last minute, there is a risk of error in procedures to verify the individual accessing the facility. Proper procedure *should* involve:

1. A proactive telephone call from the an authorized representative of the customer to initiate an access ticket
2. A follow-up phone call back to a phone number on file for the customer to verify the authenticity of the caller's location.
3. A password, challenge, or identification code to authenticate the caller.
4. The visitor's corporate (preferably photo) identification
5. A follow-up phone call to the vendor at a known telephone number on file to verify identification of the individual.
6. Ideally, a password or identification code to authenticate the vendor.

There are some significant weaknesses, which can be exploited to allow an unauthorized individual to gain access to a facility and introduce new equipment, as we'll illustrate below. Facilities enforcing the proper policies in place bear a lower risk to such an attack.

The typical social engineering attack begins with introduction and can be followed-up by a trust-building exercise, where the malicious actor builds a presumed trust relationship with the target, ending with a clandestine and undetected attack. Some examples of potentially effective scenarios include:

<u>The Phony Telecom Engineer</u>

In this scenario, the actor poses as an engineer for a company providing backbone Internet services to the facility. Data centers typically use multiple telecoms to provide bandwidth to its customers, or customers can alternatively choose their own. It is typically easy to identify which telecoms a data center is using by reading their website or contacting a sales executive. Telecoms also place premise equipment within the data center to terminate the customer side of their connections, and may even stencil their

name on conduit covers outside the building. Posing as such an engineer, an initial phone call will be made from a mobile phone or possibly even from a telecom-owned pay phone (where the caller-id will appear as the telecom's), or from any other location using a caller-id spoofer. The data center will be informed that there is an open repair ticket pending and may make up a reason, such as an alarm code sent from their equipment. Because telecoms are so large in size, follow-up phone calls may be hit-or-miss, and are frequently overlooked. Tight procedure would require a phone number on file be used for follow-up, but in many cases this information is either not stored on file or the attacker convinces the data center staff to use an alternate number. Once granted access to the facility (using a phony identification with a logo from the telecom's website), the actor is free to plant equipment in the telecom rack and possibly set up network or out-of-band access.

Phony Building Security

In this scenario, the actor is dressed professionally in a dark blazer with a walkie-talkie can easily pose as security or building personnel at some non-dedicated facilities located within office buildings. Building management for office buildings are, in most cases, required to have full access to all rooms. Because a building is responsible for electrical, fire alarms, and sometimes ventilation, individuals looking to socially engineer their way into a particular office (including a data center) might take advantage of the obscurity between building management and the data center. Using ploys such as fire alarms malfunctioning or electrical problems, the malicious individual may convince staff to grant him a guest card (for working through the problem throughout the evening) or even prop the door open. While building management typically isn't expected to introduce new equipment, a device could be concealed inside a toolbox introduced with a secondary attack (e.g. escorting an electrician with the now-trusted building manager). A smaller device could be introduced as well, possibly to simply plant on a door lock for future entries.

Phony Service Call

Because expensive equipment is typically stored within a data center, many customers purchase third-party service contracts to perform repairs of defective servers, networking gear, and other equipment. In order for the actor to pose as a phony service technician, a one would need to manufacture a false identification. This can be done with a laminator and logo from the company's website. Because most procedures do not require the customer to list all possible vendors for their facility's equipment, the attacker could pose as a technician from any high-profile company such as Sun Microsystems, Cisco, IBM, or others. This attack begins with a proactive telephone call posing as a customer, and requires knowledge of which customers are hosted in the data center facility. This information can usually be gained through discussion with one of a data center's account executives during reconnaissance, who, in order to close a sale, might drop a few names of customers hosted in the facility. If procedure is not followed and a phone number already on file (or a challenge) is not used to verify, the actor can set up access for a second actor, posing as the vendor, who will follow. This actor will be granted access to

the facility and the customer's cage, where they may introduce new equipment or sabotage the customer.

4.1 The Customer: Misdirection Over Confrontation

Fortunately, a terrorist utilizing any of these approaches has yet to be seen, however one thing is certain: it is much easier to gain legitimate access to a data center as a customer than to risk taking a chance at confronting personnel with such a social engineering attempt. Now we will move on to one of the more dangerous vulnerability in such facilities: where the attack comes from an authorized customer.

Data centers are a corporate business, and it is both competitive and financially beneficial to expedite the initial installation time for new customers. Typically, little or no requirements, other than financial and contractual obligations, are required in order to procure rack space in such a facility. Because terrorists are organized and funded, purchasing facility space is not be a problem. Many facilities will lease space for as little as $500 per month. The corporate strategy behind these facilities also caters to new business, which requires these facilities' services immediately. While some facilities have basic safeguards in place, such as refusing cash payments or signing in new equipment at the door, it is still quite simple to introduce concealed explosives or other devices into a facility as a customer. After an initial reconnaissance evaluation, the attacker may become a customer of the facility at which point a contract will be filled out and initial payment made via check or credit card. Once this is complete, the provisioning process begins and the rack space is assigned. In many cases, this entire process can take less than 24 hours.

As a business requiring privacy, confidentiality, and professionalism, a vast majority of data centers maintain a "healthy" abstraction from their customers to stave off liability for overhearing confidential information or receiving trade secrets. Certainly no background checks are performed on individuals or businesses seeking to lease rack space in a facility. In many cases a business license is also not necessary as an individual hosting personal equipment is just as valuable a customer as a business.

> **NOTE:**
> Pre-Paid Credit Cards are now available, leaving very little if any trail. Organized terrorists may not even require such cards as they may be in possession of laundered card, appearing legitimate, but be suspicious of prepaid cards. Most data centers do not have procedures in place to identify or refuse prepaid credit cards.

4.2 Introduction of Equipment

Once the attacker/customer has been given access to a data center, equipment may be introduced into the facility and bolted to the racks, hidden beneath the floor, or in a

number of other places depending on the attack. Typically, data center facilities do not open and inspect customer hardware beyond recording a serial number and description of the equipment. Most data centers also fail to require a copy of any equipment's keys to remain on the premises. An attacker can easily introduce whatever equipment is necessary without inspection. This can include explosive devices, small nuclear devices, electromagnetic devices, and etcetera.

> **NOTE:**
> I recently received an email informing me that the gamma radiation from a nuclear device will cause fiber to turn opaque. Although this can be avoided with the proper shielding, this can be a detection approach taught to staff, as most facilities have some form of exposed fiber connected to equipment. Small radiation detection devices can also be purchased to detect radiation in a room.

Due to the large and heavy nature of most enterprise class computer equipment, plenty of free space is available in any large computer chassis to accommodate such devices as well as keep them cool, concealed, and stable. The Sun E450 is an ideal example of such a chassis, as a significant amount of free space is available for drive arrays and would require little or no modification to hide such a device. Other choices may include a Cisco 12000 series router, most RAID chasses, or any large "stackable" type computer systems.

Using the serial cable or other interfaces, these devices can be connected to a computer or directly connected to one or more of the data center's Internet carriers. Some of the possible ways such devices could be smuggled in include:

- Placing them inside a large computer chassis
- Removing the hard disks from a RAID unit and using just the bay doors as cover
- Bringing in a large metal box that "looks technical" enough not to be suspicious
- Piece by piece installing several smaller pieces of equipment into a customer-owned cabinet.
- Concealing the device underneath the raised floor present in most data centers
- Concealing the device within sealed battery cases

In most cases, the device can be hidden in plain site. Once the attacker has introduced their equipment, it will generally go undisturbed by staff. A majority of facilities have no hardware inspection policies or procedures and most facility staff is forbidden to handle customer equipment except in an emergency (e.g. fire), to avoid liability. Some facilities do have very strict policies regarding exit hardware, however these do not generally extend to entrance hardware.

5. Detonation of Equipment

Data centers render timers and RF detonators obsolete. The key commodities in a data center are space and high speed Internet access. As the business involves Internet connectivity, very high-speed connections are provided to the customers. Connecting this

to the computer that has been introduced provides a remote means of detonation from anywhere in the world over any layer of encryption the attacker finds necessary. Should a small nuclear device have been smuggled in, detonating the equipment from inside the building could easily take out the city block or more. This can also be used to launch a collaborative attack involving multiple large cities as targets. Ticking bombs with daily or weekly reset switches may also be used, ensuring that isolation will not prevent detonation.

A more complex attack may include an automated scan of news sites for a threshold of matches to particular key words such as "Bin Laden Captured". Once the system has been connected to the Internet, it can be trained to detonate on any event ranging from the system date to the score at the last Yankee's game. There is virtually no way to detect such monitoring tools.

6. Possible Solutions

Now that we have discussed various vulnerabilities, let's take a look at some of the ways security can be improved in these co-location facilities. Below are some suggestions, which can help as both deterrents and detection approaches.

6.1 Unshakeable maintenance procedure

The social engineering approach to maintenance-based access hinges completely on the lack of proper procedures and authorization checks at a company. The "ignorance factor" is taken advantage of to authenticate phone calls, uniforms, and paperwork. The steps to fixing the hole in the maintenance arena include:

- A centralized maintenance management. Require all maintenance appointments, including emergencies, to go through a central maintenance manager (or group). All appointments should be logged and confirmed with the vendor (by calling them back at the phone numbers already listed for them). Emergencies should be handled in cooperation with the NOC (to confirm if a particular vendor is having an issue, there should be an open ticket) and building management. Where possible, known vendors should be assigned a verification password specific to that facility. Any technician visiting the facility should be required to give said password.
- Authentication of all telephone calls, identification, and documentation. All telephone calls into the company for maintenance should be logged, and the numbers called back before the conversation can even start. More so, the vendor should identify him or herself and be reachable at a phone number already on file. No maintenance requests should be accepted from a cellular phone. All appointments should be confirmed twice prior to allowing access. All documentation should be checked and compared with the formal documentation already on file for the particular vendor.
- Avoid informal trust relationships. This does not mean to avoid allowing the vendor to buy lunch - it is important to know the vendor as a matter of fact - but

what this means is do not establish a common familiarity with those frequently servicing the facility. Do not permit them to bring guests unless the vendor has cleared them. Confirm the individual's credentials every time they are given access to the facility (one never knows when a technician get fired and turned into a disgruntled employee, or fired for failing a background check or polygraph test).

- Supervised maintenance. A small group of individuals should be assigned to oversee any and all maintenance performed. While the individuals do not necessarily need to understand the complete technical nature of the maintenance, they must be able to identify what actions are appropriate for the maintenance being performed. For example, is a telecom vendor installing a smart jack supposed to bolt some large equipment to a rack? What does wireless equipment look like?
- Equipment and toolbox inspections. All equipment and large toolboxes, etc. entering the facility should be briefly inspected and scanned for explosives using a portable detection device or trained K-9. The individuals inspecting the hardware should have adequate knowledge to identify suspicious looking devices, and the bomb and radiation detector can do the rest of the work. There are many portable bomb detection devices on the market today, which can be used to scan all incoming equipment. An X-Ray and a metal detector can catch any smaller devices. All chasses should be unlocked and inspected internally. A majority of server chasses can be opened with a simple latch. Tight procedures for introducing new hardware presents only a temporary and one-time annoyance, but are paramount for thwarting these types of attacks.

6.2 Knowing customers

An undetected attack in this arena hinges on the ability for the individual to become a customer. The biggest problem with the co-location business is that there is not a very solid relationship between the provider and the customer. In contrast, when an individual rents an apartment, their credit and references are checked, the individual is interviewed, and based on the character of the individual, it is determined whether or not they are allowed to rent. When a new bank account is opened at a financial institution, much of the same happens, and the individual’s activity is even reported to federal agencies. Unfortunately due to the technology industry failing and in the name of privacy rights and professionalism, renting rack space in a data center usually requires no such check. The only reason many sales executives may even know what their customers do is from casual conversation and not background checks. Responsibility for the customer passes to provisioning or network operations, there is a cutoff between the data center and the customer. The customer is now a number, and no questions are asked.

All facilities should make every attempt to know who their customers are and where they've come from. Having background checks part of the standard contractual obligation reduces the chances that anyone will become offended. Visiting their place of business and learning as much about the customer are also ways to insure that you're not doing business with the wrong group. This will force attackers to build long term relationships

with their targets, establishing a corporate presence, draining their finances, and making it all the more possible for them to become exposed.

New customers should provide more specific information about their business. Are they a web hosting company or an online trading company? What do they intend to use the hardware in the rack space for? If the customer appears to be unfamiliar with their own business, this can help set off an alarm to investigate the customer more thoroughly. Some other questions to ask include:

- Does the customer have a website?
- How did they pay... cash, personal check, company check, credit card or wire transfer?
- Was their account confirmed as a business account?
- How long has their account been opened?
- Is a copy of their business license available?

Some information can be discerned from common interaction with the customer. If the company has been around for several years, have offices, and a staff then it is most likely a legitimate business (or an elaborate front). On the other hand, if the company is a new virtual company with a residential address, there is significant reason to be concerned. Data center facilities already have the liberty to discriminate based on many other criteria such as whether or not the company sends spam, broadcasts pornography, etcetera. Ensuring the customer has a justifiable business is certainly a responsible approach to accepting new customers.

6.3 Phased Provisioning

Implementing a network provisioning period that allows the customer to install their hardware before their network connectivity or POTS lines become available will give the provider plenty of time to perform any such inspections before they are given the ability to communicate with their hardware from anywhere in the world (one key ingredient to detonation). An individual who would seek to launch this type of attack would most likely do so for the purpose of executing remotely...otherwise they would simply drive a Ryder truck up to the target and commit an act of suicide.

Facility contracts should be worded in such a way to allow for a one or two-week provisioning period. During this period, all hardware inspections, background checks, and other such checks can be performed.

6.4 Tier-Level Facilities

New customers without a strong business are not likely to have the same requirements as a larger customer. Depending on the volume of rack space needed, having separate facilities will allow for lower-tier customers to be hosted in location less critical to infrastructure. For example, bottom tier customers requiring less than one full rack of space might be hosted in a lower-profile facility outside of critical areas of commerce.

This will force the complexity of the attack to increase dramatically, in order to procure space in the more sensitive locations, where an attack is more likely to cause damage. Access to these more restricted locations can, in fact, require additional background checks and other means of verification.

6.5 Non-Discriminating Hardware Inspection Policies

Basic policies regarding hardware entered into and stored in the facility can help give the provider additional means of inspecting equipment and ensuring new customers don't attempt to introduce explosive or other dangerous devices. Adding a clause to contracts requiring a copy of all equipment keys to be stored on the premises and a requirement stating the provider "reserves the right to inspect any hardware brought into the facility for malfunction or malicious use" gives the facility provider the ability to perform periodic checks of all hardware for not only terrorist conspiracies, but also to insure there are no fire risks, loose power cables, or any other facility hazard. Such a policy is easy to justify.

Explosive detection tools are available as well to scan new hardware. K-9 officers can be trained to detect up to 11 distinct odors of explosives. An occasional pass-through of the facility by a trained K-9 officer can provide a non-intrusive way to check out new customers without the need to even touch their hardware. Such inspections may even be provided at no charge as a public service by the police department depending on the area. Other actions such as checking underneath the raised floor for any devices, closely monitoring a customer's actions and behavior, and scanning the room with a thermal camera are all less intrusive ways to keep an eye out for suspicious activity. Finally, swab tests can be performed in almost any setting to detect explosive residue.

Paying attention to the kind of hardware the customer brings in is another good way to identify suspicious activity once the account executive builds a relationship with them and knows their business. Is the user a dialup Internet provider? Why do they not have any dialup access equipment such as modem banks? Are they a web hosting company? Why do they have only one large server instead of several small ones? Is the traffic they are pushing commensurate to the business they are running and the amount of bandwidth they purchased? Are they pushing any traffic at all? As small as they are, these inconsistencies can pile up and help to identify a customer who is not really who they say they are (even if one is just looking for spammers rather than terrorists).

6.6 Continual Monitoring

Monitoring the amount of throughput is a good way to identify dormant systems, which may exist only for a one-time communication before detonating. Data center facilities selling high-speed connections should be suspicious of any customer who is pushing very little data. Traffic patterns consisting of low bandwidth and a spike at a specific hour of the day may also be a sign of automated triggers scanning other systems for news or any external trigger. Further inspecting traffic on an IP level can identify the number of

distinct hosts the customer's equipment is communicating with. A very large amount of equipment communicating with a very small number of hosts is at the very least suspicious.

6.7 Restricting Building and Rooftop Access

Many facilities providers allow their customers to network to the roof of the building where antennas or satellite gear are mounted. Restricting this type of access to where the customer must be accompanied by staff during normal business hours will help prevent any "soft target" attacks on the building or surrounding area.

If the facility is located in the same building as a targeted corporation, or if there is a possibility of a different style of attack (for example, a release of biological toxin from the roof top), the individual may attempt to use this opportunity to attack in other ways. By having 24-hour access to the data center, the attacker may also have 24-hour access to the entire building. Having a building security guard monitor the status of individuals in the building will help detect if a customer who is supposed to be on the 10^{th} floor is snooping around on the 4^{th} floor. Ventilation ducts, stairwells, and telecom closets are all viable means of concealment and mobility and should frequently be checked and secured. Policies for introducing new equipment outside of normal business hours can be implemented requiring permission from the facility provider. Additional steps similar to these can and should be taken to secure the building outside of business hours.

> **NOTE:**
> In some states, such as New York, laws exist requiring that rooftops to any Federal builds be secured.

6.8 External Self-Assessment

Hiring an outside firm to test the effectiveness of the policies a company has in place for knowing/choosing their customers and managing the facility will help expose any loose individuals in the company. Hire a firm to create a company with some suspicious ties and send actors to carry out a mock attack. Do they succeed? What about equipment policy violations? Can they effectively pose as a maintenance technician and gain access? A terrorist isn't likely to be walking in with guns blazing and take over the building, but rather play a game of invisibility and misdirection, taking advantage of the very nature of "good-willed" or ignorant individuals...these external tests can help identify these weak areas.

7. Conclusion

Data centers are an ideal terrorist target. It is of the utmost importance to take the necessary steps to protect these facilities from an attack. Detecting the vulnerabilities in these facilities is the first step. Once they are exposed, finding an effective plan to fix procedure and inspection will help make the facility a secure place of commerce rather than the next target of attack.

Security for these facilities is ultimately left up to the facility maintainer. The FBI may be able to help improve the security of such locations by cooperating to assist in detection and defining policy and procedure.