Written for the Business Recovery Managers Association
October 2000 (Note: Prior to Sept. 11)
Eugene Tucker, CPP, CFE, CBCP

Data and Network Security-The Basics: Physical Security

It makes little sense to invest thousands of dollars in firewalls and intrusion detection software when someone can simply walk out the door with your server (this has happened more often than one would think). The understanding of how to identify vulnerabilities and how to protect your data begins with the basics of physical security.

People rank the compromise of their personal information as a greater fear than domestic terrorism although there has been much more loss and injury from these crimes than from credit cards compromised over the internet. Perhaps for this reason, many network administrators, who forget that most network intrusion attempts are internal, first concentrate all of their initial efforts protecting against those lurking in the cyber bushes. In spite of the availability of automated cracking tools that require a lesser degree of technical know-how, I was recently told it is often easier and more effective to pay the janitor to connect a laptop and sniffer to the proper connections in a router closet. In many small companies, you can just walk in and simply connect to any network jack and gain ownership of the system.

Larger corporations, especially those that would suffer high losses resulting from intrusions, are beginning to combine the corporate security functions with those of IT security, and often business continuity planning, under a single director. In companies without this capability, the responsibility (but usually not the authority, staffing, or budget) may fall within the area of BCP. If the network is down due to a virus, denial of service attack, spray painting, or just someone tinkering around, it becomes our duty to recover from the situation and therefore to identify the risks and to mitigate their effects. If your firm has a security professional on staff or someone charged with this responsibility, work with this person to address your vulnerabilities and concerns. If not, utilize a corporate or physical security consultant to cover the basics. As a last, and cheaper resort, there are several books available that contain checklists of what to look for, but usually don't do a good job telling you how to correct a deficiency found on the list. Increasing, these lists cannot protect the firm from security liability issues.

Security is a simple concept-more an art than a stringent set of formulas and procedures, that identifies and anticipates the possibility of attack and eliminates or reduces the opportunity for it to occur. It is often an attitude or a way of looking at a facility or process based upon experience and research on vulnerabilities and types of criminal methodologies. An understanding of why crimes (and intrusions) are committed or not committed (prevention) is important. Prevention through the fear of identification (capture) and its resultant negative consequences are major contributing principals. Security measures are designed to **deter** the criminal, **detect** their presence, **delay** the

attack thus increasing the probability of capture or discouraging continued attack, and **denial** of access to the target. Remember that one purpose of security is not to protect against someone with an intent to do damage, but against someone with a good intent but not the knowledge or responsibility to affect a system change.

When designing a security program, many of those responsible simply begin to implement what they see or read about at other facilities. This is often a waste of resources and may not address vulnerabilities of data networks (although may be good from a physical security liability point of view). When setting up or auditing a physical security program, first think in broad terms to identify vulnerabilities and then drill down to more specific risks. Step back from your facility. Look at it as a target and yourself as a data thief. How, as an outsider, can you get in without detection long enough to accomplish your goal? Don't actually try this of course. Can you simply climb over a fence or fake an ID badge? There is a story in the security world, probably true, of a company executive who wanted to test the attention of his guard force by placing a picture of a monkey over his own picture on his employee badge. Each day of the week the employee was waived through the door by the guard after the executive held the picture up so it was plainly visible. Finally, out of frustration, the executive asked the guard if he noticed anything different. The guard simply replied, "Oh, you shaved." This story illustrates just how easy it can be to walk into many facilities.

Physical security is often thought of in terms of 'rings of protection': the outer ring, the perimeter of the property, can be 'protected' by fencing or other barriers, cameras, bright lighting, security patrols, conceptual and environmental design. The next level may be the outside of the building itself. Proper locks on doors and windows, control of landscaping around the building, alarm systems, tight key and access controls (i.e. guards and/or card readers; employee, visitor, and contractor identification) are important protections at this level. The next ring would be internally focused around specific things you need to protect. Care to guess how many times the author has simply walked into an unlocked data center? Answer: too many-some did not even have locks. Like passwords, install locks (cipher locks or access card readers are good) and change combinations often and always after a data center employee leaves the company. Card readers can generate an audit trail of who and when someone entered the room. Ensure no one can climb over the wall of the data center through a false ceiling or interstitial. Avoid 'advertising' the location of the data center with display windows (who wants to see your poor cabling habits?). Equip all distribution frames and router closets with self-closing doors that remain in a locked (from the outside) position. Check to see if power systems are secured. Although not always possible, do not allow janitors or others to share space with your equipment.

In addition to physical security, it is important to implement a program that checks into the background of prospective employees and more importantly, of those vendors and strategic partners that have access to the data, networks, or equipment. Work with risk management or legal to implement or audit an intellectual property protection program. The loss of trade secrets or other corporate intelligence can cost the company more than a week's worth of downtime. Audit the physical security of partners that share trusted

access to important systems and audit the security of your off-site storage facility. Will they deliver or issue back-up tapes to those not authorized? Do they perform their own background investigations of employees to determine there are no conflicts of interest?

Take steps to protect the theft of laptop systems:

- Use anti-theft devices that lock the laptop to the docking station or to the work surface. Do not allow users to keep keys in the docking station.

- Install tape-recorded CCTV to view all exit doors. Consider the use of covert cameras.

- Establish access control policies and install access control equipment. This includes strict control of who is allowed to enter the building after hours. Restrict access to areas of the building where laptops are located. Access control devices such as card readers should generate a record of who entered the building. Restrict access and egress to and from the building to the fewest doors possible. Install panic alarms on doors designated as emergency exits only.

- Encourage employees to report suspicious activity.

- Consider marking laptops with the name of the company in bright letters. This could make the resale of the computer difficult.

- Never leave laptop computers unattended when traveling. Beware of schemes designed to grab your laptop as it comes out of the x-ray machine at the airport. Have it hand inspected if possible.

- Install theft detection software that identifies the laptop and phone number it is connected to.

Hopefully, this information will allow you to take one of the first steps toward the protection of your valued information. Keep checking your BRMA library for books, CDs, and other resources on this topic.