Keep your business information assets safe

Part IV: Addressing your Physical Security

This is part four of a four-part series that identifies business information assets, helps business owners understand the value of their information and then explains how best to protect information as a valuable business asset.

To quickly recap our previous articles in the first article we discuss the value of information, how to establish that value and the cost the impact a lost of information can have on the financial stability of your organization. We introduced the concept of ROSI (Return on Security Investment) as a way of evaluating the investment in security as it relates to the potential cost of lost information assets. We also examined the total cost of a security breach including how to establish the value of the information and the cost of repair and recovery of lost or compromised information assets.

In our second article we examined the impact of organizational attitude has on the protection and integrity of your information. We talked about how and why development of a security information plan is important and the need for good policies and procedures that are properly communicated to employees. Finally, we discussed the issues of audit and enforcement and how important that is to the insuring a safe and security information infrastructure that allows your staff to utilize systems effectively while at the same time protecting those critical information assets from inappropriate access and usage.

In our last article we addressed the technical issue of security; we identified the different technical components, how those components work to together insure a secure environment and finally the concept of a holists approach to technical security.

We now come to the final element in protecting your information assets, physical security. We have established that your information has value to you and if lost can have a major negative impact on your ability to operate or even stay in business. Next we know the role and responsibility of management to establish an organizational structure that provides best practices for protecting and security your information. And finally, we examined the role the technology plays in providing the tools to protect and manage the security of your information. The best security in the world from an organizational and technical viewpoint is worthless if the door is left open. Physical security one of those things that is both new and old, new in that new technologies assist us in better controlling physical access and old in that the basic issues haven't changed. Controlling who gets in and out, when and where.

Not only does physical security deal with access it also addresses health and safety of your business and staff. Some of the issues addressed in physical security are as follows:

1. Access control, who is allowed where and when, this includes issuing and tracking of access devices, i.e. keys, cards, etc.
2. Fire protections, including monitoring, suppression and training.
3. Employee protections, both external from outside threats such as criminal elements and, in this day and age, terrorist, and internal from all forms of abuse, including physical, harassment and drugs.

Physical security requires you to look at your organization from a different viewpoint. Too many people become lax in their own physical environment; they begin to accept little things around them and don't look with a critical eye. Example, several years ago I performed a risk assessment for a large client. This client had two secure data centers. The data centers were placed next to each other with a

common wall. In reviewing the data centers I noted several things, first, all the servers were logged in with administrative passwords without any screen locking, to this comment the client felt they didn't need to worry about this since only authorized personnel were allowed in the data centers. Upon further investigation I noted that the two data centers, one with motion detectors and cameras, had not only a common wall but the first one shared a common wall with the first aid room and that the ceiling tiles over the data center had been removed to facilitate the data cables. The crawl space over the whole area was around twenty feet high. This demonstrates how two dimensional people are. They hadn't thought beyond the horizontal and hadn't considered that someone could enter the first aid room (open to all staff and visitors) crawl up over the common wall, enter the first data center and access any of the servers, or crawl over the second wall and defeat the security system and access the highly secure second data center and servers.

This points out how the security conscious technical staff had been oblivious to a physical security threat. Physical security must carry the same importance and weight as the technical or organizational security issues.

In this day and age, physical security also includes protection of the employees from harassment and threat, ask yourself, do you have a harassment policy in place, how do you handle anger in the workplace, what is your policy when an emergency occurs?

These questions need and should be answered, if not you are possibly placing your employees in danger.

(Caroline need something here to wrap up the series, ideas?)