Security management

Business, Management

There are quite a lot of types of coercion that can influence the safety of an enterprise and the property it plans to guard. It is up to management to understand these different threats and ensure that the proper countermeasures are implemented. For a company to properly protect itself and its assets, it must implement the correct security management practices (Harris, 2002). An overall approach to security management is needed to address a wide range of issues, including workplace violence.

Often, HR managers have responsibility for security programs, or they work closely with security managers or consultants to address employee security issues (Mathis & Jackson, 2006). Functions Management should dictate the role that security will play within the company. They should define the scope, objectives, priorities, and strategies of the company's security program. It is their responsibility to get security off the ground, support it, and ensure that it is properly maintained. Without senior management's support, a security program will not usually have the necessary attention, funding, and resources.

Also, security recommendations are usually not taken as seriously if employees do not perceive that they are supported and enforced by upper management. Senior management also has an overall understanding of the company's business, vision, goals, and direction, and they should use this insight to direct the role security will play in the company. Without management taking the lead, there is usually a lack of direction regarding computer, information, physical, and personnel security, and any efforts usually fail before they truly start (Harris, 2002).

Security management lets a manager maintain and distribute passwords and other authentication and authorization information. Security management also includes processes for generating, distributing, and storing encryption keys. It can also include tools and reports to analyze a group of router and switch configurations for compliance with site security standards. One important aspect of security management is a process for collecting, storing, and examining security audit logs. Audit logs should document logins and logouts (but not save passwords) and attempts by people to change their level of authorization (Oppenheimer, 2004).

Theft and Shoplifting Theft or larceny is defined as the taking of another person’s property without permission with the intent to deprive the owner of the property. Auto theft and shoplifting are two examples of theft. Most jurisdictions classify the crime of theft according to the kind of property taken or the value of the property taken. Theft may also be an additional crime is another incident, such as theft after burglary of a residence or business. Most calls of theft are received as past incidents. A caller notices that certain property is missing and has no idea what happened to it.

In the case of auto theft, the call may be received very soon after the actual theft occurred. Shoplifting calls may involve a shopkeeper who has apprehended a shoplifting suspect (Emergency Telecommunicator, 2001). Unfortunately thief and shoplifting go on in a volunteer operated shop as well as the retail shop in the mall. In fact, volunteer operated shops are often targeted for thief and shoplifting. The shoplifter thinks that the volunteer

manning the shop is an easy target and that even if he is caught most likely the organization will not prosecute.

Policies on thief should be adopted by the organization and carried out (Kirk, 2005). Retail Loss Prevention The retail business is afflicted by costly thievery that is perpetrated by criminals both inside and outside the company. It’s an affliction that adds up to as much as $60 billion a year in the United States and to a proportionately staggering amount in Canada. Obviously this must have a significant effect on the cost of doing business and this on consumer prices. Loss prevention methods have been improving but they – as well as our attitude toward shoplifting – still have a long way to go (Robinson, 1999).

This figure masks the true cost of crime prevention, because prevention of crime, such as employee recruitment methods and screening; investment in staff retention and reduction in employment of part-time staff; and training in retail crime and security plus supervisory and management skills. Retailers know that motivated, trained and retained staff can reduce customer and staff theft, in addition to spotting and dealing efficiently with external threats to security (Fernie & Moore, 2003). A partnership must exist between management and employees dedicated to protecting the company assets.

While no one method is the cure-all, employee awareness, training, and reinforcement do help reduce losses. Theft by employees can have a serious effect on the profitability of the company, thereby limiting corporate opportunities. Corporations with strong values and ethical mission

statements usually have an active approach to the protection of company assets and ensure that a safe and honest work environment exists. Every employee must be educated about company policy regarding theft and the consequences from the beginning. This “ indoctrination” or orientation should begin even before the employee is hired.

During the interview process and the prehiring procedures, the employee applicant should be made aware that the company has a strong concern for employee honesty, “ shrinkage,” and “ shortages. ” Let applicants know how the company feels about business abuse will not be tolerated (June, 2000). The best way that a volunteer manning the shop can discourage and reduce shoplifting is to greet each costumer with eye contact. Persons contemplating shoplifting who know that they have been seen are less likely to commit the crime, for fear of being identified.

The volunteer should be instructed in the proper way to handle a shoplifter. For safety of the volunteer and the liability of the organization they should never approach the shoplifter or accuse them in the shop. The volunteer should actually witness the shoplifting/theft and then call security to apprehend the shoplifter outside the shop. In an alert, fully staffed shop, placement of the shop’s fixtures and securing expensive items will deter shoplifting (Kirk, 2005). Solution A key part of security involves controlling access to the physical facilities of the organization.

Many workplace homicides occur during robberies. Therefore, employees who are most vulnerable, such as taxi drivers and convenience store clerks, often are provided bulletproof partitions and restricted access areas. Many

organizations limit access to facilities and work areas by using electronic access or keyguard systems. Although not foolproof, these systems can make it more difficult for an unauthorized person, such as an estranged husband or a disgruntled ex-employee, to enter the premises.

Access controls can also be used in elevators and stairwells to prevent unauthorized persons from entering designated areas within a facility (Mathis & Jackson, 2006). Current Technologies A variety of tools exist for maintaining security logs, including Event Viewer on Windows 2000 machines, syslog on UNIX and Cisco IOS devises, and C2 auditing for detailed audit reports on UNIX systems. The US Department of Defense defined C2 security, including auditing, as part of its guideline for computer security (Oppenheimer, 2004). Burglary systems are what people traditionally think of when they think of security systems.

Although security professionals understand that a comprehensive physical protection system is usually much more than a burglary system, this technology still has a prominent place in the protection of assets (Vellani, 2006). It is important to choose a theft-prevention system early in the planning process. The architect will need to know the specific placement requirements to allow for successful installation of the system’s components. Electrical wiring for the theft-prevention system can be installed in several ways. In new construction, the cables can be buried in a raceway under the finished floor.

This method is best in terms of both appearance and eases of maintenance and requires exact installation specifications. Alternative installation

methods require routing the cables in a surface-mounted raceway or on an aluminum threshold on the floor’s surface (Kirk, 2005). Conclusion The importance of establishing an enterprise-wide security program in company organizations is well recognized. Such a program must have top management support and direction if it is to be successful. The program must be supported by sufficient resources to accomplish its goals of protecting informational privacy and integrity and ensuring data availability.

An adequate security perspective places all of these consequences with the countermeasures design. The scope of the security program must be sufficiently broad to encompass all vital organizational information systems and resources. An appropriate organizational structure must be established to ensure that adequate policies and procedures are developed, implemented, and monitored. As the business establishment moves toward more automation and integration of internal and external data sources, the importance of security programs as an integral part of the organizational structure will be continue to be recognized.