Effective Data Center Physical Security Best Practices for SAS 70 Compliance

In today's ever-growing regulatory compliance landscape, organization can greatly benefit from implementing viable and proven data center physical security best practices for their organization. Recent federal legislation, ranging from the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and The Sarbanes Oxley Act of 2002 (SOX) are putting intense pressure on data centers, co-locations, and managed services entities to comply with a myriad amount of security and privacy issues. What's more, companies seeking to use services from data centers are actively looking for assurances that a strong control environment is in place, complete with data center security best practices. These best practices, which many times are tested by an independent CPA firm for SAS 70 Type I or Type II audit compliance, should be implemented throughout all areas of a data center, rather than being segmented to cover only specific areas. The SAS 70 auditing standard, in place since 1992, has been and will continue to be one of the most effective and well-recognized compliance audits for testing and reporting on controls in place at data centers

Data Center Physical Security Best Practices Checklist

From the moment an individual walks through the data center doors, the following items should be part of a data center physical security best practices program for any data center building:

- **Built and Constructed for Ensuring Physical Protection**
  The exterior perimeter walls, doors, and windows should be constructed of materials that provide Underwriters Laboratories Inc. (UL) rated ballistic protection.
- **Protection of the Physical Grounds**
  The data center should have in place physical elements that serve as battering rams and physical protection barriers that protect the facility from intruders.
- **Bullet Resistant Glass**
  Certain areas within the data center, such as the lobby area and other entrance mechanisms, should be protected by bullet proof or bullet resistant glass.
- **Maintenance of Vegetation**
  Flowers, plants, trees and other forms of vegetation should be appropriately maintained for purposes of not allowing these elements to conceal or hide an intruder.
- **Security Systems and 24x7 Backup Power**
  The data center's security systems should be functioning at all times, complete with uninterruptible power supply (UPS) for ensuring its continuous operation.
- **Cages, Cabinets and Vaults**
  These physical structures which house equipment must be properly installed with no loose or moving components, ultimately ensuring their overall strength and rigidity.

- **Man Trap**
  All data centers should have a man trap that allows for secure access to the data center "floor".
- **Electronic Access Control Systems (ACS)**
  Access to all entry points into and within the data center should be protected by electronic access control mechanisms which allow only authorized individuals to enter the facility. Included within the framework of electronic access control should also be biometric safeguards, such as palm readers, iris recognition, and fingerprint readers.
- **Provisioning Process**
  Any individual requesting access to the data center should be enrolled in a structured and documented provisioning process for ensuring the integrity of the person entering the facility.
- **Off-boarding Process**
  Personnel working for the data center or clients utilizing the facility services must be immediately removed from systems that have allowed access to the facility itself. This includes all electronic access control mechanism along with removal of all systems, databases, Web portals, or any other type of sign-in mechanism that requires authentication and authorization activities.
- **Visitors**
  All visitors must be properly identified with a current, valid form of identification and must be given a temporary facility badge allowing access to certain areas within the data center. This process must be documented in a ticketing system also.
- **Alarms**
  All exterior doors and sensitive areas within the facility must be hard wired with alarms.
- **Cameras**
  The facility should have a mixture of security cameras in place throughout all critical areas, both inside and out, of the data center. This should include the following cameras: Fixed and pan, tilt, and zoom (PTZ) cameras.
- **"Threat Conditions Policy"**
  Consistent with the rating scale of the Department of Homeland Security, the facility should have a "threat conditions policy" in place whereby employees and customers are made aware of changes in the threat.
- **Badge and Equipment Checks**
  Periodic checks should be done on employees and customers regarding badge access and equipment ownership.

- **Local Law Enforcement Agencies**
  Management should have documented contact information for all local law enforcement officials in the case of an emergency.
- **Paper Shredding**
  A third-party contractor should be utilized for shredding documents on-site, then removing them from the facility, all in a documented fashion, complete with sign-off each time shredding is done.
- **Data Center Security Staff**
  These individuals should perform a host of duties on a daily basis, such as monitor intrusion security alarm systems; dispatch mobile security officers to emergencies; monitoring to prevent unauthorized access, such as tailgating; assist all individuals who have authorized access to enter the data center; controlling access to the data center by confirming identity; issue and retrieve access badges; respond to telephone and radio communications.
- **Additionally, they should also conduct the following activities:**
  Response and resolution to security alarms; customer assistance for cage lockouts and escorts; scheduled and unscheduled security inspections; enforcement of no food or drinks on the raised floor area; Enforcement of no unauthorized photography policy; fire and safety patrol inspections.

Facilities interested in complying with these data center physical security best practices in the context of a Type I or Type II audit will benefit by learning the history and overview of the auditing standard, along with important facts and SAS 70 benefits.