WCRE
WOLF COMMERCIAL REAL ESTATE

#InformationFriday

PHYSICAL SECURITY CONSIDERATIONS

By David J. Humphreys, MS, Security+, CISSP CTO & Principal Security Consultant, Avasek November 4, 2016

When most think of cyber security focus is directed toward the virtual world and not physical security. However, for a complete security program it would be foolish to overlook the physical aspects of cyber security. This paper will serve to some as guidance to regulatory compliance and others as good general best practices for ensuring the security of critical data.

When thinking about the "security" of your data it is important to understand what issues need to be considered. The CIA Triad is a model designed to guide policies for information security within an organization and addresses the confidentiality, integrity, and availability. Confidentiality is typically the first association a personal makes when thinking about security, which is roughly equivalent to privacy. Integrity deals with maintaining the consistency, accuracy, and trustworthiness of data. Availability is achieved through regular maintenance, maintaining necessary system upgrades, providing adequate bandwidth, backups, among others.

With a better understanding of the CIA Triad, let's apply this to multi-tenant buildings. Many multi-tenant buildings have shared services when it comes to the maintenance of the building. Janitorial staff, maintenance services, electrical services, and sprinkler systems are just a few examples of shared services. How can you ensure that CIA of your systems in a shared service environment? How are you going to protect your equipment from water damage because of a fire in a neighboring suite that triggered the sprinkler system? If you share an electrical panel with neighboring suites what measures have you taken to make sure a surge from someone else's doing doesn't impact your business operations?

Computer equipment is expensive and vital to your business operations. It is imperative that you take measures to protect it. Identifying a location to centralize all of your networking and server equipment so be carefully considered. There should be no windows because of security and sound. A separate air conditioning zone or a wall mount system will ensure that temperature control is maintained. Class A fire resistance ceiling tiles should be installed into the server room and the floor below if above the first floor. 2 or 3-hour fire rated drywall should be installed on all four walls of the server room to minimize the risk of damage. Dedicated electrical circuits should be installed from the electric panel to the server room. If more than one electric panel exist, then a circuit should be installed from each so that dependencies on an individual panel.

Many of the above recommendations may be difficult to implement on a pre-existing structure, however, when moving they can be considered when deciding on an office. Outside of those recommendations there are easy-to-implement controls as well. Most are intrigued with the mysteriousness of sophisticated hacking capabilities

follow us:

"Building Successful Relationships" is our Mission.

Wolf Commercial Real Estate
www.wolfcre.com

NJ OFFICE
951 Route 73 North | Suite D
Marlton, NJ 08053
P 856 857-6300 | F 856 283-3950

PA OFFICE
630 Freedom Business Center | 3rd Floor
King of Prussia, PA 19406
P 215 799 6900 | F 610 768 7701

but in reality most attempts are done with much less sophistication such as watching over someone's shoulder as they log into a site or simply looking at one's computer monitor. I was at my children's orthodontist office, which has an open floor plan with individual stations consisting of a dental chair and island that houses the medical supplies and computer for their EMR. The problem is that I can be sitting in the chair for my child's appointment and take pictures of the computer screen to my left or right for other patients being seen while pretending to surf the internet. The moral of this story is that all information system output devices (monitors, printers, audio devices, etc.) need to be positioned away from general traffic to prevent unauthorized individuals from obtaining the output.

In conclusion, no one can deny the challenges that we face these days when it comes to security. Prioritizing risk management is becoming a necessity and will ensure that your business has the resiliency to withstand the unexpected.

For more information contact:

David J. Humphreys, MS, Security+, CISSP
CTO & Principal Security Consultant
phone: 856.316.4144 x103
Email: david@avasek.com

AVASEK
Protecting your critical data

follow us:

"Building Successful Relationships" is our Mission.