INFORMATION SECURITY: THE PROPERTY MANAGER'S CRITICAL ROLE

By Brandon Kriner, CPPM, Northern Virginia Chapter

Information security is becoming increasingly important in a time when data is becoming harder to protect. Advances in technology have increased the storage capacity and portability of devices that store data. Many organizations are focusing exclusively on the IT challenges of information security in the wake of high-profile data theft incidents. Encryption and virtual private networks are effective shields against unauthorized access, but a comprehensive security plan must also include the physical security of mission critical data. Property managers can help keep their organizations safe by increasing awareness of and accountability for the assets that store sensitive material.

Take a look around your office. How many highly portable assets do you see that could be used to capture and transfer sensitive data? Laptops and personal digital assistants (PDAs) come most readily to mind, but today's workplace is awash with items like flash drives, recordable CDs and DVDs, MP3 players, external hard drives and camera-equipped cellular phones that are capable of storing valuable, sensitive information. These items are often classified as non-accountable because of their low acquisition cost, but the nature of the data stored on an employee's flash drive can quickly change its value to the organization.

Many property managers have considered the task of accounting for low-value property as an unnecessary burden. FAR part 45.101(a) defines low-value property as "Government property…with an acquisition cost of $5,000 or less." However, sensitive property is one of several classes that are specifically excluded from this definition. Inexpensive ADPE devices have not traditionally been considered sensitive property. The result is an accountability vacuum in which thousands of flash drives and PDAs containing priceless data lack essential physical controls. The near-ubiquity of these devices requires property managers to take a new look at the scope of sensitive assets.

The FAR defines sensitive property as "property for which the theft, loss or misplacement could be potentially dangerous to the public safety or community security, and which must be subjected to exceptional physical security, protection, control and accountability." This definition certainly applies to data storage devices, yet sensitive asset controls have traditionally focused on non-technology items such as weapons and explosives. In today's world, the security of laptops and other devices has become just as important as the security of hazardous materials. Moreover, many flash drives, cellular phones and MP3 players are the personal property of employees and thus not subject to the same controls as organization-issued laptops and PDAs. Property professionals, along with their counterparts in IT, need to increase organizational awareness of the changing scope of sensitive assets and the importance of individual efforts to safeguard these items.

Property managers must capitalize on the increased focus of physical data security by providing greater accountability for storage devices. All organization-issued property capable of storing computer-readable data should be designated as sensitive in the property system. Accountability for all data storage devices in the property system provides decision makers with a complete picture of the organization's exposure to risk from sensitive assets. Accurate property records also ensure personal accountability and capture valuable data for investigators in the event of loss or theft. For example, the model and serial number were instrumental in the correct identification and recovery of a recently stolen

Department of Veterans Affairs laptop. Police were able to use data from the Department's property records to distinguish the laptop from others for sale in a pawnshop.

Extra controls for data storage devices should be implemented to prevent loss and theft in the first place. Property passes should be issued and checked for all data and storage devices taken off the organization's premises. Physical inventories of sensitive assets should be conducted with greater frequency than inventories of non-sensitive assets to ensure the prompt discovery of missing items. Sensitive assets that are not found during inventory should be subject to a formal internal inquiry process before being written off. A police report should be filed as soon as reasonably possible if an asset is reported lost or stolen by an employee. Finally, sensitive assets should be overwritten, degaussed or destroyed prior to donation, sale, or abandonment.

In today's world, the nature of sensitive assets has changed, but the mission is still the same: provide accountability and control for the proper use and care of property. Property professionals now have the opportunity to provide a crucial line of defense against a devastating leak of sensitive data. We must do more than simply keep our organizations out of the headlines. Our obligation is to protect the well being of thousands of people who depend on us to keep their information safe. Protecting property is necessary, but protecting people is the most important responsibility of all.

Biography:

Brandon Kriner, CPPA is a business analyst for Sunflower Systems and has over five years experience in property management. Brandon has an MBA from Johns Hopkins University, MD and a BA from American University, Washington, D.C.