TECHNICAL UPDATE

CTSI
Serving Colorado's Counties

Volume 26 Number 51 December 20, 2022

Securing & Disposing of Data

An organization can be held liable if its data is improperly accessed. This applies to portable data tools such as cell phones, laptops, or hard drives. There have been several large data breaches caused by lost or stolen equipment, such as the theft of a Veterans Affairs employee's laptop containing sensitive data for 26.5 million veterans, their spouses, and active-duty military. A recent survey revealed that one-quarter of employees have reported lost or stolen smartphones, and 81% of companies have reported losing laptops with confidential data. There are steps you can take to limit the damage done should equipment with sensitive information fall into the wrong hands.

SECURE DATA

Any electronic equipment connected to the internet is at risk from viruses, hacks, or ransomware. A virus on a network-connected device could potentially destroy the general system, so anti-virus and security software should be required on all devices. Password-protected entry should also be required. Consider using a multifactor authentication (MFA) process to enhance device security. Also, limit employees' ability to put confidential information on mobile devices—human resources staff, for example, do not need remote access to such data. Employers should have specific protocols for authorizing confidential data on mobile devices, and wireless devices should not access confidential information off the network.

Centralize desktop applications in a secure data center, so only one location needs to be secured. When giving telecommuters and other employees remote access, deploy technology that automatically locks out a device if a virus or breach occurs, so one employee's computer problem does not impact the entire company.

DISPOSING OF ELECTRONICS

A comprehensive information security policy should cover properly disposing of out-of-date devices. There are three basic steps to safely and securely dispose of computers, printers, or other equipment that contain drives with data:

- Ensure you have copies of the data from the source being destroyed
- Securely wipe the drive using either the DoD 5220.22-M protocol that writes over the hard drive data three times or the newer NIST standard. Tools, such as DBAN, exist that can implement these or other standards.
- Dispose of the computer or equipment properly. If the equipment is not being recycled, physically damage it to ensure nothing can be read from the drive. This is especially important if the computer or equipment is damaged and a software-based secure erase cannot be performed.

WHAT THIS MEANS FOR COUNTIES

Counties should minimize the risk of harm from data loss and data falling into the wrong hands by taking security measures such as keeping track of all mobile devices, limiting remote access, and disposing of equipment properly. When an employee who was issued a smartphone or laptop returns it or when a device is being replaced, all data should be stripped from it. For more information, contact CTSI at 303 861 0507.