Cyber Security April

From the County Network Security Cooperative

PHYSICAL SECURITY – What is it?

According to an article by Michael Cobb from Tech Target, “physical security” is “the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, terrorism, and possibly personal harm.
Prioritizing damage prevention avoids the time, money and resources lost because of these events.

Access Control

Access Control is a physical security measure to limit and control who has access to sites, facility areas and materials. Access control encompasses the measures taken to limit exposure of certain assets and locations to authorized personnel only. To gain access through government barriers, ID badges, keypads, and an integrated intercom with a camera can allow a receptionist or guard to open a barrier and allow access.

Surveillance-Using Technology

Surveillance using technology can encompass the use of cameras, heat sensors, moisture sensing devices, and other notification systems. Many surveillance systems can be integrated with access control. Threat actors who see an IP camera are less inclined to break in or vandalize a building out of fear of having their identity recorded. Similarly, if a particular asset or piece of equipment is stolen, surveillance can provide the visual evidence one needs to identify the culprit and their tactics.

Purchase Hardware that complies with Federal Statutes

When purchasing access control and surveillance for a government agency it is a good practice to vet the product manufacturers your agency is considering. The link provided will guide you to a listing of products from the FCC that are deemed to pose unacceptable cyber security risks.

Link: https://broadband.nebraska.gov/FCCCoveredList

Testing and Verification

Physical security is a preventative measure and incident response tool. Disaster recovery (DR) plans, for example, center on the quality of one's physical security protocols.

Regimented testing is the best way to ensure that such policies and procedures pertaining to Access Control and Surveillance Footage will be effective when an incident arises. A crucial part of this is to verify your access control logs and video footage are properly backed up.

Keeping a record of what is accessed—and what people attempt to access—is a reliable way to not only discourage unauthorized users but create a forensic-friendly data environment.

The County Network Security Cooperative is a collaboration of partners including:

Nebraska Association of County Officials

NIRMA Serving County Government

Disclaimer: This document reflects current guidance and is subject to change due to the evolving cyber security environment.