Reflection Paper

Katherine Chang

Old Dominion University

CYSE 368: Cybersecurity Internship

Theresa Duvall

Over the last 50 hours, I have been involved in enhancing the physical security of the technician's office at NASA, which stores critical hardware. The focus was on ensuring that sensitive equipment is adequately protected from unauthorized access.

My Center Operations Manager (COM) began by reviewing the office's current entry control systems and identified areas where additional measures were needed. This led to the installation of more secure locks and the integration of biometric access controls for higher-security areas within the office. They also implemented a system for logging visitors and restricting personnel access to maintain proper tracking of hardware and sensitive materials. Though we were not experiencing issues where assets were going missing, from a security perspective, we should have had stronger security in the technician's office, especially with assets being stored there prior to deployment.

As part of the security enhancements, a locked cabinet was implemented to securely store mobile phones and their accessories. This measure was introduced to prevent unauthorized access to devices that have not been deployed yet. The cabinet is equipped with keys that are only accessible by me. Additionally, a logging mechanism was established to track all transactions (notating in the tickets which techs have requested/picked up hardware), ensuring accountability and facilitating audits.

Figure 1Mobility Cabinet

Figure 2 Badge reader for tech office