

Organizational Factors and Descriptions

The following organizational factors may encourage or present opportunities to potential malicious insiders.

Access and Availability



- Acquisition: The availability and ease of accessing and acquiring proprietary, classified, or other protected materials, such as providing access privileges to those who do not need them.
- Removal: The ease with which someone may exit the facility or network system with proprietary, classified, or other protected materials.

Policies and Procedures



- Policies: Undefined policies regarding working from home or during unscheduled times on projects of a sensitive or proprietary nature.
- Prevention: A lack of security procedures or monitoring to prevent theft or misuse of information and materials.
- Labeling: Incorrect or nonexistent labeling of proprietary, classified, or controlled information or materials.
- Lack of training: Employees are not sufficiently trained on how to properly protect sensitive or proprietary information and materials.

Time Pressure and Consequences



- Time pressure: Employees under time pressure may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.
- Consequences: The perception that security is lax or the consequences for theft or other malicious activities are minimal or non-existent.

Source: Federal Bureau of Investigation