



JULY 2008

Securing Vault-type Rooms

The use of vaults and vault-type rooms (V/VTRs) and other security containers are regulated for good reason: they are the first line of defense in protecting the classified matter stored within. But as this case illustrates, physical controls are only as effective as those trained and entrusted to use them. If users do not follow the procedures that are in place, the security system can fall apart.

Case

Recently at around 6:00 pm, a Central Alarm Station (CAS) end-of-day report showed that vault-type room (VTR) #1 was not alarmed. A check of the VTR found it unoccupied, locked but not alarmed, and the building unoccupied. Protective Force called in the VTR custodian, who determined there was nothing missing from the VTR and there was no sign of unauthorized entry. The custodian secured the VTR. The log showed the VTR was last opened at 2:15 pm by Joe. The Security Container Check Sheet (SF 702) showed Joe opened the VTR at 2:17 pm and closed it at 4:16 pm. Joe's co-worker, Ernie, then verified the closure at 4:17 pm. No name appeared in the "Guard Check" column of the SF 702. A review of the Protective Force phone records showed no call between 4:00 and 4:30 pm to alarm the door as the site procedures required. During the security inquiry, Joe said that after he finished his work about 4:10 pm, he properly locked and alarmed the VTR. He exited the VTR, logged out of the access computer, closed the door firmly, checked to ensure it was latched, and spun the dial on the lock. While Ernie was double-checking the door, Joe called the CAS and provided the required information to alarm the VTR. Joe said the Protective Force security officer, whose name he did not write down, told him that the VTR was alarmed. Ernie, however, did not recall seeing or hearing Joe call CAS to alarm the door. Joe was adamant that he had properly closed and alarmed the VTR.

Security Concern

The VTR was locked but unalarmed and unattended for about 90 minutes, during which time someone with the VTR combination and badge access to the building could have accessed the VTR and the classified information in it.

Causal Analysis

Joe properly locked the VTR and had it double checked. He failed to follow procedures and call the CAS to alarm the VTR.

EVER WONDER WHAT EVENTS
LEAD UP TO A
SECURITY INCIDENT?
CSI CAN UNRAVEL THE
CLUES.

CSI:
CONTEMPLATING
SECURITY
INCIDENTS

EXPLAINING WHAT A
SECURITY INCIDENT IS
AND HOW IT UNFOLDS.



ISSM Focus: Step 4 – Perform work within security controls.

Controls had already been developed and widely used in VTRs, but Joe failed to follow the established procedures either because he was in a rush at the end of the day or allowed himself to be distracted.

Work securely.

Corrective Actions

Joe and his entire group were retrained on how to properly secure a VTR. Joe's division established policy requiring those calling the CAS to write the name of the CAS operator on the SF 702. The division trained all its workers on this policy and established a weekly check to ensure the procedure was being used.

Infraction

A security infraction was not issued to Joe because:

- the incident was immediately self-reported through the appropriate channels;
- Joe had not been found at fault in a security incident in the two years prior to this incident;
- the incident did not adversely affect security interests because the VTR was properly locked, the VTR logs showed no entry in the time it was unalarmed, there was no indication of unauthorized entry, and no material was missing; and
- Joe cooperated fully in the inquiry.

Lesson Learned

- Double-check your work. If you perform any task routinely, it is very easy to assume you had done something even if you had not.
- Writing the name of the CAS operator alarming the VTR on the SF 702 can ensure the person securing the VTR does not miss this crucial step.
- The Protective Force's policy of recording calls to the CAS was an effective tool in determining the cause of this incident.