SECURE OPORD

Several minutes have passed after the crew worker finished his smoke break. The bravo team member who bummed a cigarette from him earlier rapped three times on the external door and the other bravo team member llets him in. The area is partially lit, but free of the cleaning crew. Operational orders in the RoE say they must reach the server room and retrieve an external hard drive left for them by the client stakeholders.

Hugging the darkened wall, the bravo team makes their way toward a pair of French doors they believe leads into the main office corridor. Upon reaching the doors, they rush the hallway stopping every few seconds, still not knowing where they are until one of the team notices a sign saying: IT Department. AU enclosed offices and room are centered in the middle of the building. Bravo team rushes each enclosed office/ room until. one operator notices a room protected by a PIN pad. One operator inserts the borescope under the door. It looks like the rigiht room, but it's dark. The other operator removes the curled up under-the-door tool from his bag and moves it into position. Quietly the operator pops the door latch! They move in quietly, switching to NVGs. It's the server room. Sitting on a server in an open rack is the external hard drive. Kneeling on the raised computer room floor, server fans whirring loudly, cool air circulating and LED lights flashing everywhere, the bravo team radios the red team leader, "Red team leader, this is bravo team. Objective 2 reached!"

Secure OPORD is a significant phase, if not the most significant phase, of the REDTEAMOPSEC methodology, or any given physic.al red team operation for that matter. It Is at this point where the red team carries out the intended actions on objective.

By this time, quite a bit of activity has occurred. Reconnaissance has been performed, the team has staged, moved into offensive position, exploited physical weaknesses, and gained access into the facility. Now comes the time where the all-important objectives are carried out It's all led up to this.

Execution

Mission Goals							Recon Results		
	Goal	Plan	Mission Success	Estimated Vulnerability	Threat	Bad Actor	Observations	Vulnerability	Go-Forward?
1	Gain unauthorized access through a loading dock to capture evidence and leave a business card.	Deploy from area #1, approach from rear van, move west along alley wall. Wear black tactical gear and use under the door tool and air wedge to gain access. Capture video evidence and leave business card.	Gaining access via door exploit, capture evidence, leave business card and exfiltrate without detection.	Inadequate perimeter security.	Moderate to significant service disruption.	Local to regional bad actor. Moderately sophisticated.	Loading dock traffic is moderate by day, non-existent by night. No cameras visible, have motion lights. No RFID badge entry, only door locks. External doors have ADA levers and weather stripping below.	No motion alarms. No security cams. Motion lights can be bypassed on east side. ADA lever handles could be bypassed with under-the-door tool and air wedge. Infiltration to happen at night.	Yes.
2									

Sample Mission Goals

As I mentioned in an earlier chapter, part of the Execute Staging phase is to reassure every red teamer fully understands what constitutes mission success and how to get there. Figure 85 is taken from planning documents. Inside the Mission Goal is precisely where the OPORD lies and is paramount to the success of the mission.

Let's start on the right of the figure; it shows output from reconnaissance efforts under the heading, Recon Results.

Mission Goals		Recon Results		
	Goal	Observations	Vulnerability	Go-Forward?
2	Gain unauthorized access and retrieve a piece of equipment to simulate a physical data breach.	Side entrance traffic is used by smokers moderately by day, minimal by night crew. No cameras visible, no motion lights. No RFID badge entry, only door locks that appear to be left unlocked by night crew.	Night cleaning crew leaves door open to take smoke breaks leaving the facility vulnerable to equipment theft, tampering, IP theft, and physical data breaches.	Yes

Recon Results (some columns hidden)

Recon Results

This section includes three columns that aim to provide a bit of history from the recon team. This is a helpful reminder to the execution team in the event recon was done by another team. Let1s break down this section a little more.

Observations

In this example, the recon team identified a side entrance that is used by smokers, during the day by employees and at night by the cleaning crew. The night cleaning crew had a habit of leaving this door unlocked during their shift. The recon team also stated they did not see any cameras, motion detectors, or RFID readers. We know from the story at the start of a previous chapter that the bravo team found an RFID reader had been instal.led between phases, throwing a giant wrench into their plan.

Environments are constantly changing. While it may seem to some the client in this case should have told the red team a new security control had been installed, that is almost always not the case. This is partly the reason for the Assess & Acclimate phase, and even then, some things will go unnoticed.

Vulnerability

As a result of the observations the re con team made earlier in the operation, here they indicate what is believed to be a vulnerability. Because the night cleaning crew leaves the door unlocked, it gives rise to the potential for theft of equipment, tampering, intellectual property theft, and overall physical data breaches. The Observations and Vulnerability columns combined tell a short story about the physical. security posture and potential vulnerability identified.

Go-Forward

In the Go-Forward column, the recon team indicates 'Yes' or 'No' on whether this suspected vulnerability is one that deserves to be tested as a mission goat In our example, the observation here turned into a fuU-fledged mission goal due to the gravity of the vulnerabillity.

Mission Goals

Mission Goals				
	Goal	**Observations**	**Vulnerability**	**Go-Forward?**
2	Gain unauthorized access and retrieve a piece of equipment to simulate a physical data breach.	Side entrance traffic is used by smokers moderately by day, minimal by night crew. No cameras visible, no motion lights. No RFID badge entry, only door locks that appear to be left unlocked by night crew.	Night cleaning crew leaves door open to take smoke breaks leaving the facility vulnerable to equipment theft, tampering, IP theft, and physical data breaches.	Yes

Mission Goals (some columns hidden)

Starting from left to right in the figure above are the columns most relevant to the execution team. This data is what's most useful during the latter phases of the REDTEAMOPSEC methodology, especially this one.

Goal

> *"Gain unauthorized access and retrieve a piece of equipment to simulate a physical data breach."*

The Goal column provides a brief summary of the objective. I find this data to be most important to client stakeholders. It should be written so that it is easily consumable at a high level. There should be no technical jargon here.

Plan

This column is a summary of the salient action steps the red team will be conducting. It briefly states what, where, and how the team intends to reach the goal as advertised in the Goal column.

From our story about the bravo team, we know there has been some deviation from the plan. We know the RFID reader forced the team to improvise and the plan changed. This is to be expected, and the important thing to keep in mind is that the deviation was not significant enough to be considered out of scope. A character change (clothing) and social

engineering were planned, but not in the way the team had originally planned.

Mission Success

The Plan column indicates what, where, and how, but the Mission Success column defines under what circumstances the goal is considered successful. The red team must gain access, retrieve a "fl.ag" (external hard drive), and exit unnoticed. This provides additional parameters on how the goal must be achieved.

> *"Gain access to facility, find server room, gain access, retrieve an external hard drive, and exit unnoticed."*

Plan and Mission Success language shoul.d be written with flexibility in it to allow for slight deviations when unexpected issues arise. Even though the bravo team had to improvise on their feet, the spirit of the plan did not change significantly, according to the language. Therefore, mission success for this goal had been reached.

Mission Goals			
	Est. Vulnerability	**Threat**	**Bad Actor**
2	Inadequate perimeter security and employee / contractor security awareness.	Moderate to Significant business impact.	National to Regional bad actor. Moderately Sophisticated.

Mission Goals (some columns hidden)

Estimated Vulnerability

Here we more formally and categorically define the vulnerability. As opposed to the Vulnerability column in the Recon Results area, which is more narrative, the language here serves to support what would typic.ally accompany language in a typical security finding. Categories like this are used to better organize findings that are subject to remediation efforts and

also to help clients understand which categories need the most improvement.

Threat

The Threat column is relatively straightforward and brief. This communicates to clients the perceived threat to the organization as a whole.

Bad Actor

The Threat column is relatively straightforward and brief. This communicates to clients the perceived threat to the organization as a whole.This column indicates how sophisticated a would-be attacker would need to be in executing this goal successfully. It also indicates if the bad actor is more likely to be local, regional, national, or international.

Again, the OPORD provided in the Mission Goal. is at the heart of the operation and must be fully understood in order to effectively reach mission success.

SITREP

We know from earlier in this book that a SITREP is a situational report used to notify senior-level leaders of a tactical situation and status usually occurring after a significant event. It is a short and concise statement and, in a physical red team operation, is usually broadcast over a two-way radio to the red team leader. The red team leader may request a SITREP on an ad-hoc basis as well.

The red team leader uses the information relayed in a SITREP throughout an engagement to make critical decisions regarding the operation as a whole.

However, the SITREP following an operator having reached a mission goal. during this phase, as in the story at the start of this chapter, is the pinnacle of an operation.

It is at this point, and this point only, after having received a SITREP that the red team leader, in her position of operational power, declares

mission success, mission failure, or otherwise. But before we get into the specifics of other outcomes, allow me to provide a simple SITREP template for operators to use.

There is no requirement to adopt military radio etiquette. The SITREP template here is merely an example a team can use to efficiently communicate. At such a pivotal. point in the operation, this is one area where your team may want to utilize military radio etiquette if you have not already done so.

MISSION STANDING

When things go right, the red team leader will announce mission success, in response to the SITREP, and order the team to exit the target. It is usually evident when a mission has successfully reached its objectives. The red teamers know it, and the red team leader gives the order to exit. But things don't always go as planned. Sometimes mission objectives aren't reached or sometimes they take longer than expected. Sometimes operators are compromised, and mission success turns into mission failure.

Here are a few red team leader mission orders:

- **Resume OPORD.** The red team leader grants additional time for the team to attempt to secure OPORD.
- **Concede.** For example, if an operator is compromised by an employee, the red team leader will give the order to show authorization letters, ID, and forfeit the mission.
- **Abort.** The red team leader believes the objective can't be reached and orders the team to move on or exit the target entirely.

It is important for the team to know the meaning of these orders and what to do. The most common of these for my team is resuming OPORD. Chance, randomness, and surprises tend to pop up more than we plan for, and it seems mission goals take longer than we anticipate. Operators should provide SITREPs to the red team leader when encountered with unplanned issues that delay the OPORD process.

Conceding often happens when operators are spotted by employees, guards, or law enforcement.

In the case of employees, operators should always attempt to social engineer their way out of a sticky situation. A pretext and character change, as I mentioned in Chapter 11, should be used to further those efforts. Conceding to employees should only be done when it appears that no way out is possible.

When confronted with law enforcement, on the other hand, the process should be handled much differently. Any and all operators must immediately concede in the event they are compromised by an officer. This means providing authorization letters, government-issued ID, and complying with the officer's commands. Do not lie, run, or hide from law enforcement. I repeat, do not lie, run, or hide from law enforcement. You could be putting yourself into grave danger, let alone serious legal ramifications.

Aborting a mission goal is prone to happen and it shouldn't be frowned upon. It's probably a sign that the client is doing things right. In a physical red team operation, there are almost always a multitude of mission goals. Not every goal can be or is expected to be reached. Aborting all mission goals, on the other hand, is a different story altogether.

I imagine there are a few scenarios where aborting the entire operation is necessary, though I've never been a part of one that has. However, physical injury and law enforcement intervention fall well into that category.