RED TEAM ASSESSMENT CASE STUDY

ANDREW WHITMER

SecureState

Table Of Contents

Security, Responsibility, and Accountability

Many, if not most, organizations compartmentalize their security efforts in the same manner they compartmentalize different business functions. For instance, information technology may perform account management, facilities and maintenance may distribute and track physical keys, and human resources may conduct initial or recurrent user awareness training.

Leaders and managers are familiar with the truism that one can delegate authority but not responsibility. Indeed, in large and complex organizations, some degree of delegation is always necessary. Unfortunately, when security-related tasks are divided between different departments, accountability becomes difficult to track and enforce, and ultimate responsibility is unclear.

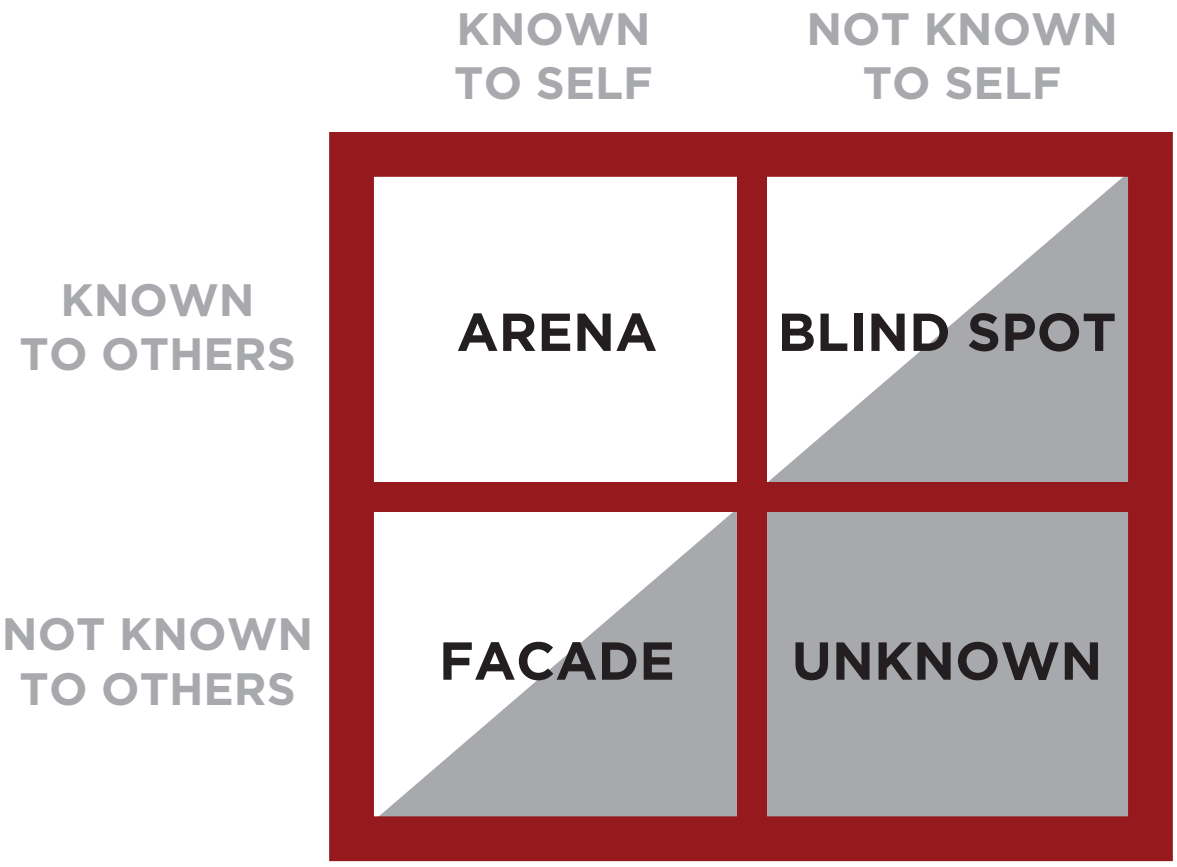
This is because the different departments, which are generally siloed with independent reporting channels, may have inconsistent perceptions of the scope of one another's responsibilities. In the context of security, this compartmentalization can lead to gaps in policies and practices. This problem can be exacerbated by excessive reliance on specific security engagements which do not view the organization or its security holistically. For instance, an external penetration test can do an excellent job of identifying vulnerabilities in an organization's external defenses; however, it does not necessarily illustrate how these vulnerabilities may be leveraged outside the scope of that specific assessment.

The Unknown Unknowns (The Johari Window)

When fissures appear in an organization's security program due to gaps between departments, they can go perilously unnoticed. This is because the independent departments do not have the purview or insight to look beyond their own boundaries. Since the gaps exist between departments and disciplines, organizations are not always equipped to identify them, leading to unknown issues and blind spots.

In February 2002, then Secretary of Defense Donald Rumsfeld popularized the phrase "unknown unknowns," which he described as things "we don't know we don't know." Though Rumsfeld's press briefing reintroduced this concept to contemporary political culture, it goes as far back as 1955, when psychologists Joseph Luft and Harrington Ingham presented the Johari Window.

The Johari Window

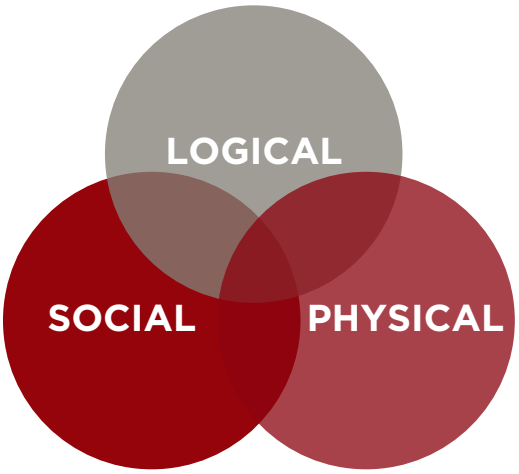


Though the Johari Window was developed to help people understand themselves and their relationships, it provides a useful framework for organizations to consider their relationship with their security programs and the gaps or vulnerabilities therein. The danger, of course, lies in weaknesses that are not known to the organization itself. As long as gaps in security are also unknown to others, the organization can enjoy some measure of security through obscurity. Unfortunately, through meticulous reconnaissance, probing, and actual attacks, an organization's adversaries can – and will – uncover gaps that the target organization is unaware of, turning these "unknowns" into "blind spots".

Even after being discovered by an outside force, these exposures often remain unknown to the organization. This is a reflection of the reality that motivated and sophisticated attackers do not compartmentalize their attacks in the same manner that organizations compartmentalize their defense. Nor do attackers enforce artificial distinctions between different areas of security, such as physical and logical. Attackers do not care whether the method of compromise is an unlocked door or an unlocked workstation – both present perfectly viable methods of access. Furthermore, real attackers do not honor narrowly defined scopes or normal operating hours, and will target an organization's weakest links.

Train Like They Fight

Organizations seeking to truly protect their information, rather than simply check a box or complete a required audit, should acknowledge the reality their adversaries know – security is a comprehensive discipline and requires comprehensive testing. SecureState's approach to uncovering these blind spots is the Red Team assessment. A Red Team assessment provides a threat-representative simulation of an attack in which outsiders attempt to acquire access to an organization's sensitive data. This assessment conceives of security in three domains – social, logical, and physical.



Attacks in the social domain use social engineering to target the organization's personnel. If successful, these attacks - which may occur through email, over the phone, or in person – may result in more information, access to computer systems, or even physical access to facilities. Logical attacks are launched with and through information systems, which could take the form of bruteforcing accounts or exploiting vulnerabilities in publicly facing systems. These attacks generally result in access to computer systems and the information therein. Physical attacks exploit vulnerabilities in physical security controls to gain access to sensitive areas, systems, or information. A physical attack could be as simple as jumping a fence, or as complex as cloning and reusing an access badge.

Unlike organizations that artificially (if inadvertently) attempt to isolate these domains, attackers relish scenarios in which these domains overlap. This is the modern, criminal equivalent of the combined arms approach in which attacks occurring across the different domains have mutually beneficial effects. Where attackers see an opportunity, targeted organizations often see nothing, because the attack targets their blind spot.

As an example, an attacker may drop a USB drive with a malicious payload in a location where it is likely to be found. If inserted into a user's machine, the payload calls back to the attacker, providing them with remote access into the organization's network – a social attack in the physical domain providing logical access. That access may be leveraged to target the organization's access control system by adding a new card – a logical attack providing physical access. That physical access could be exploited to compromise the target organization's sensitive areas and information.

Organizations that attempt to compartmentalize these security domains and responsibility for them are less likely to identify these complex attacks.
Moreover, they are also poorly positioned to respond to the attacks, because they lack the necessary protocols, communication channels, and inter-departmental insight. These structural limitations also mean organizations struggle to close the gaps in the wake of an attack.

Though the example above is hypothetical, it is representative of those engagements which SecureState has conducted for organizations across a variety of industries. One such assessment, performed for a client responsible for elements of national critical infrastructure, provides a case study of how vulnerabilities within one domain can be leveraged in another, and how procedural and communication gaps between the domains provide blind spots from which attackers can launch dangerous attacks.

Breaking in through the Johari Window - A Case Study

As an electric service provider, the target organization (OBJECTIVE JONAS) had undergone numerous vulnerability scans, penetration tests, and physical security assessments over time. A user security awareness program was also in place. However, the organization had made the strategic decision to view its security posture cohesively, and knew that these piecemeal assessments would not ultimately accommodate that strategic vision. Therefore, it enlisted SecureState for a Red Team assessment, setting trophies of employee PII and physical and logical access to certain critical systems.

Logical Domain

SecureState began the assessment by conducting remote network reconnaissance on OBJ JONAS as well as open source intelligence (OSINT) on the business and its personnel. These activities were both passive – such as innocuous browsing of publicly accessible websites – and active – such as scanning to identify services and exposures which may not be readily visible.

The passive reconnaissance activities identified numerous OBJ JONAS employees, their positions, and contact information. Photographs and newsletters provided insight into past and upcoming events, employee identification badges, and overall company culture. This type of information is vital for developing pretexts for social engineering attacks and gathering valid accounts whose passwords may be brute forced or even guessed.

Though the passive reconnaissance was productive, SecureState's active reconnaissance activities were quickly detected and thwarted. Despite using a distributed network of systems from which to probe the target network, our offending IPs were quickly identified and blacklisted by the organization. This speaks to a level of relative maturity and investment in security around the perimeter. It is worth noting that while automated systems are often adept at blocking malicious traffic such as this, if they do not generate alerts reviewed by humans, the organization may miss an opportunity to correlate an increase in threat activity across the domains.

Having probed the perimeter in search of exposures and vulnerabilities, a typical external penetration test may have ended there. But a real attacker would simply use the information gathered from this initial sortie to reevaluate the plan of attack.

Social Domain

OSINT gathered during remote reconnaissance fed directly into a targeted social engineering campaign. Having identified the organization's remote access technologies, SecureState spoofed a login portal and sent an email to likely users of the technology. This email was forged to appear as though it had been sent from a technology administrator identified through OSINT and was timed to coincide with actual events of concern to the organization.

In truth, though the email and login portal were convincing fakes, this is a relatively standard social engineering attack with which security practitioners should be familiar. However, simpler is better at times, and in this case starting simple allowed SecureState to assess the organization's baseline social engineering detection and response capabilities. Moreover, the purpose of a Red Team assessment is not to discover and exploit 0-day vulnerabilities and launch never-before-seen attacks – the purpose is to show how dedicated, real-world attackers may exploit and link together otherwise isolated vulnerabilities to achieve a compromise.

SecureState's counterfeits resulted in the harvesting of several pairs of legitimate user credentials. However, not long after the email was sent, a handful of adept users alerted the information security department to the attack, and in turn, those users were encouraged to change their passwords. As was the case with the perimeter defenses, this line of action speaks to a level of maturity and awareness within the organization – even within our small sampling, users spotted the suspicious email and knew who to contact.

Unfortunately for OBJ JONAS, some of the affected users did not have a complete grasp of security best practices and changed their passwords in a predictable manner. SecureState maintained access to this small subset of accounts throughout the assessment. Having sent a convincing phish, tracked the results, and monitored the response, a typical social engineering engagement may have ended here. But the credentials which SecureState had acquired had much more potential than that.

Physical Domain

With the remote logical and social attacks resulting in only moderate success, SecureState traveled to the organization to explore the possibility of a physical breach. Thorough close-target reconnaissance revealed the location and orientation of cameras, the use of badge-controlled access systems, and elements of employee culture, such as tendencies to hold doors open or confront unidentified strangers. Close proximity to the organization also gave SecureState the opportunity to probe the wireless network. Though SecureState was able to crack the passphrase, the wireless network appeared segmented from sensitive internal systems.

SecureState investigated public entrances to the offices but found them well monitored and defended. Like the external network perimeter, OBJ JONAS had identified these areas as exposures and likely avenues of approach, and had installed the appropriate defenses: a staffed reception desk facing the entrance, multiple cameras with overlapping sectors of coverage, a mantrap entryway, and access-controlled doors combined to serve as effective deterrents. However, dedicated attackers (as opposed to opportunistic criminals), and those seeking information instead of money, are unlikely to attack such strong points. SecureState continued probing the organization's facilities in an effort to identify a weak link. After methodical and deliberate reconnaissance, SecureState located an avenue of approach to a maintenance facility near OBJ JONAS's headquarters. The route provided reliable ingress and egress, bypassed detection by any cameras, allowed for the caching of equipment, and reduced chances of being encountered by any personnel.

After close of business and under cover of darkness, a small SecureState detachment used this route to reach the facility's fenced perimeter. Basic tools allowed SecureState to scale the fence and probe the inner perimeter for a means to breach the facility. Ultimately, SecureState was able to open a door, granting access to the facility's interior. Though the entrance triggered an alarm, the responder did not sweep the building, providing SecureState with the time it needed to complete the compromise.

A physical site assessment or penetration test would have stopped at this facility breach. However, for the Red Team, physical access is just another piece of the puzzle.

Into the Breach

In this case, the physical access turned out to be the missing piece. It provided SecureState with access to network-connected workstations, and the opportunity to leverage information gathered from attacks launched in the logical and social domains.

One of the accounts to which SecureState had retained access was still valid, allowing the breach team to log on to a domain-joined workstation in the facility. Though the physical breach occurred in the very late hours of the night, SecureState had a separate team located offsite prepared to leverage any level of network access provided by the breach team. This team-based approach allows SecureState to replicate the basic infrastructure that a sophisticated or dedicated attacker may have and to reduce the time between the identification of a vulnerability and its successful exploitation.

The breach team executed preconfigured payloads on the workstation to which they had achieved access. These payloads called back to the remote exploitation team, who promptly began efforts at lateral and vertical escalation within the domain. Network access had been the primary objective of the breach team, and upon positive confirmation of access from the remote exploitation team, the breach team conducted hasty site exploitation before retreating. Within a matter of hours – before personnel from the organization returned to work the next morning - the remote exploitation team had achieved domain compromise and acquired PII for most of the organization's personnel.

No More Half Measures

Despite the organization's points of strength – around the external network perimeter, in response to phishing, and around the public entrances to its facilities - the "combined arms" or interdomain approach of the Red Team assessment still resulted in compromise of the some of OBJ JONAS's most vital information and that which it had set as its trophy for the assessment. This is the value of the Red Team assessment – its ability to uncover blind spots across the entire breadth of an organization's security controls, policies, and procedures, while illustrating the true risk exposed by those gaps. Moreover, the threat-representative approach allows the organization to test its detection and response capabilities in a manner that is as true-to-life as that which any assessment can provide. It is often a shortcoming in organizational security that departments lack the imagination to foresee these kinds of scenarios; without the ability to think like a criminal, gaps will inevitably arise. The best approach to security is to take a single exposure and pose the question, "How could this be used against us?"

A typical external penetration test would have identified users and exposed services but stopped at the network perimeter. A social engineering assessment may have tracked clicks, identified susceptible employees, and monitored the organization's response, but not have illustrated the risk associated with the harvested information. A physical penetration test or assessment would have identified weak points in perimeter defenses and controls that were not operating as intended, but not explored the true risk associated with them. An internal penetration test may have identified issues that allowed the exploitation team to compromise the domain, but not explained how outside attackers could have achieved an initial foothold.

Only through the execution of a holistic security test, such as a Red Team assessment, can organizations truly understand how isolated vulnerabilities can correlate and compound with one another to lead to additional, unexpected areas of compromise. By conducting an assessment that seamlessly traverses the different domains of security, an organization can gain insight into how its approach to security has left gaps and blind spots. Once these are uncovered, the organization can then take substantive steps to achieve a greater level of maturity within its security posture. Security is a comprehensive discipline that requires comprehensive testing. Attackers know this; it is time their targets know it, too.