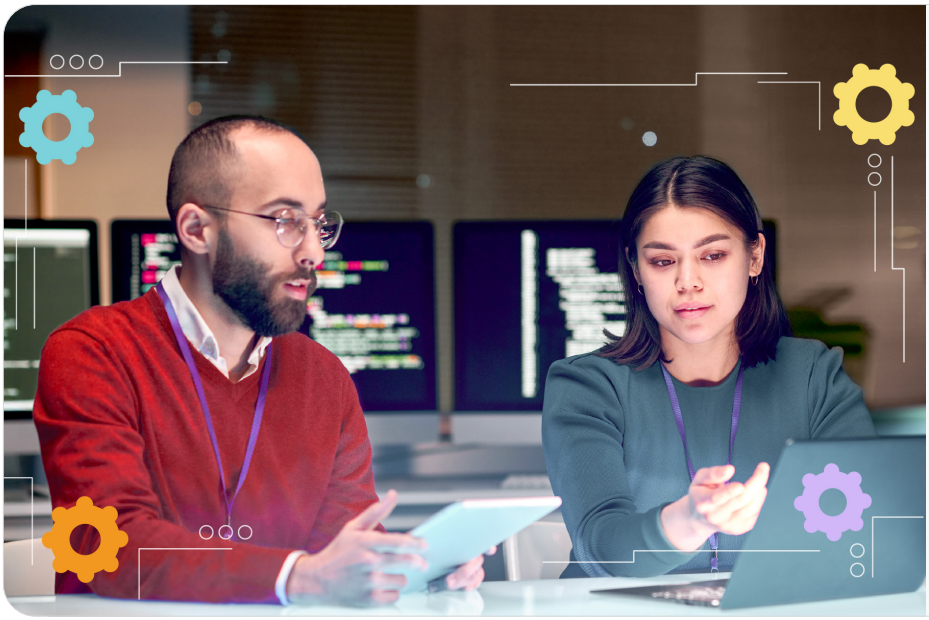
Community Bank Identifies Security Gaps with Successful Red Team Assessment



INDUSTRY
Financial Services - Community Bank

CHALLENGE
After adding new locations and staff, a community bank aimed to test its defenses against real-world threats, particularly social engineering attacks.

RESULTS
The SBS red team successfully gained unauthorized access and pinpointed critical security gaps. These findings led the bank to boost its security training and incident response protocols and to make red teaming a key part of its future plans.

SERVICE
Red Team Services

$680M+	Midwest	2	5
ASSET SIZE	LOCATION	BANK BRANCHES TESTED	WEEKS OF TESTING

> "As our bank has begun to expand, we felt it was necessary to not only test our current staff but the newly acquired staff as well. I have had a working relationship with SBS since 2017, and SBS has always taken care of me."

— Information Security Officer
Community Bank

The Challenge

Putting Protocols to the Test: A Real-World Security Challenge

This $680 million+ community bank had previously partnered with SBS CyberSecurity for compliance-based security assessments and is proactive in strengthening its security posture to protect customers' sensitive information. After acquiring new locations and personnel, the bank wanted to test its defenses in a real-world scenario — particularly against social engineering threats.

Confident in its robust security protocols, especially in high-security areas like server rooms, bank leadership decided to put their assumptions to the test. Frontline staff has received comprehensive security awareness training, emphasizing the importance of verifying authorized personnel and escalating suspicious activity. However, leadership acknowledged that new employees might not yet have internalized these best practices, leaving a potential gap in the human layer of security. To address this concern, the bank engaged SBS to complete a red team assessment, a strategic move to gauge the bank's resilience against persistent physical intrusions, phishing, and remote attacks.

While open to various testing methods, the bank set clear boundaries, excluding lock picking and RFID badge cloning. Rather than focusing on isolated technical vulnerabilities, they wanted to assess the organization's ability to detect and respond to a sustained security compromise attempt.

While the client was especially interested in understanding risk across newly acquired locations, this testing was scoped to begin with two existing branches, including the option to expand to newly acquired locations if the red team encountered strong resistance.

The Solution

Proactive Security Measures Uncover the Unknown

Preparation for the assessment began immediately after the paperwork was completed, with SBS CyberSecurity's network security engineers forming a red team to conduct reconnaissance on the bank. They identified key vendors, including the managed service provider (MSP), and gathered intelligence to support their attack. Leveraging open-source intelligence (OSINT) sources like Google Maps and social media, they mapped out entry points and high-value targets (HVTs).

With intelligence in hand, the team initiated physical impersonation at locations where IT staff were less likely to be present, reducing the chance of credential verification. At the first site, one team member operated a command-and-control console off-site while another posed as an IT technician requesting server room access for a network upgrade. After initial hesitation, an employee granted access, allowing the installation of a rogue network device that remained undetected for more than two weeks. Though the bank's MSP later flagged the device, no action was taken, revealing a critical incident response gap.

At the second location, an employee initially granted the red team access but grew suspicious and confirmed with leadership. This led to the team's removal and highlighted inconsistencies in security awareness across branches.

The team also launched phishing and phone-based social engineering attacks. A phishing attempt using a malicious Word document failed due to employee vigilance. However, a follow-up phone impersonation attack succeeded when an employee granted unsupervised remote access to a workstation. This allowed the red team to access sensitive customer information and employee data, achieving their primary objective.

Each infiltration step was documented, culminating in a formal exit meeting where the SBS red team presented findings and recommendations to bolster the bank's security posture.

> **"The team was in constant contact with me from the planning phases to ensure they had a full understanding of the expectations, asking how far we would like them to go during testing, and following up before the final reporting was completed to make sure we were fully satisfied. We were very pleased with the results and look forward to continuing this relationship with SBS."**
>
> — Information Security Officer

The Highlights

Challenge	Solution
Employees granting unauthorized access during physical and phone attacks	Enhanced social engineering awareness training and identity verification processes
MSP identifying rogue device without escalation	Improved incident response with real-time alerts and clear escalation protocols
Sensitive data accessed with low-privilege account	Implemented stricter role-based access control and time-limited permissions

The Results

Turning Eye-Opening Findings into a Roadmap for Stronger Security

The red team assessment highlighted critical areas for the bank to improve:

- **Employee awareness and response:** Despite having security training, employees granted SBS engineers unauthorized access in three separate instances — two during physical impersonation attempts and one through a phone-based attack. This demonstrated a need for more targeted social engineering awareness training, including new hires at acquired locations.

- **Incident response gaps:** While the MSP identified an unauthorized device on the network, no action was taken, allowing an attacker to maintain network persistence. This underscored the need for real-time alerts and clear escalation procedures.

- **Access control and least privilege:** The team exfiltrated sensitive data using a low-privilege user account, emphasizing the need for stricter role-based access control and time-limited permissions.

Despite these challenges, the assessment also confirmed the bank's strong defensive measures on the technical front. Operators struggled to establish long-term persistence, as automated security controls actively terminated unauthorized processes and blocked common remote access tools. This reinforced the effectiveness of their endpoint protections but underscored the importance of improving human-based defenses.

Upon learning the extent of the red team's access, the client valued the real-world insights. Leadership acted swiftly to bolster security, committing to:

- **Enhancing security awareness training** with a focus on social engineering threats and verification processes

- **Limiting exposure in a breach scenario** by implementing stricter access controls, reinforcing the principle of least privilege

Additionally, impressed by the results, the bank plans to incorporate SBS CyberSecurity Red Team Assessments into its security strategy for future expansions, ensuring new locations undergo rigorous testing before opening.

Ready to get started?

sbscyber.com/contact-us