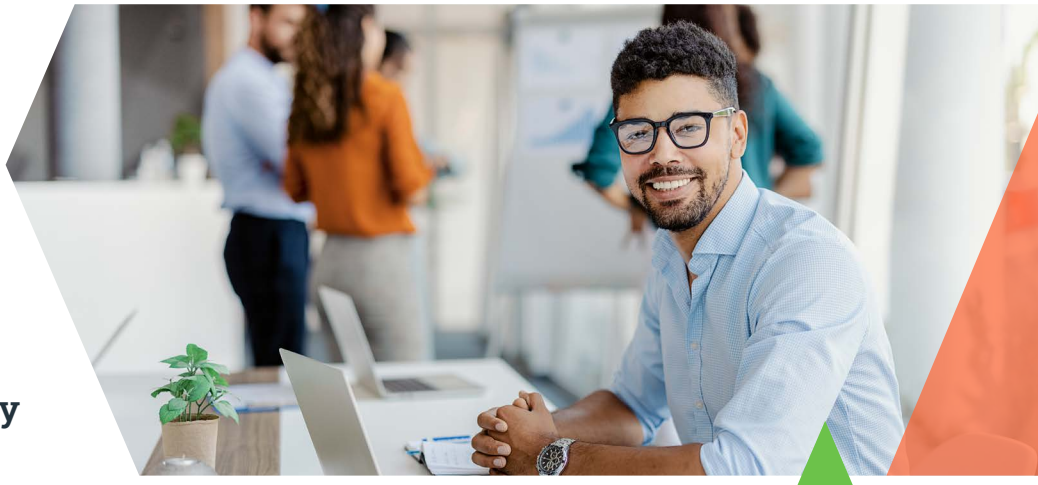
TEVORA™

Case Study



Tevora's Adversary Simulation Services Helped a Leading Global Bank Identify Vulnerabilities in Their Environment

Protecting your valuable resources against external threats has never been easy, but with adversaries continuing to ratchet up the sophistication of their attacks, it's more challenging than ever. In today's environment, attackers use a carefully orchestrated combination of advanced social engineering, physical penetration, and cyberattack techniques to find and exploit vulnerabilities in corporate environments.

In this case study, we'll explain how Tevora's Adversary Simulation Services helped a leading global bank identify and remediate vulnerabilities in its environment that were open to sophisticated attacks.

To protect our client's confidentiality, we'll refer to them by the fictitious name of International Banking Corporation (IBC).

New CSO Concerned About Vulnerabilities

In 2021, IBC hired a new CSO to replace a long-standing security executive that was retiring. Before joining IBC, the new CSO had built a strong track record at another global bank, where she had significantly strengthened its defenses against external attacks. She was proud of the fact that there had been no successful compromises during her seven-year tenure as CSO and was highly motivated to repeat this success with IBC.

One of the first things the new CSO did was conduct interviews with executives, managers, and key staff in IBC's security and privacy organizations. Her initial assessment after these interviews was that many parts of IBC's environment were well defended, but others appeared vulnerable to external attacks.

Tevora Engaged

Based on her positive experience working with Tevora before joining IBC, the new CSO engaged us to use our Adversary Simulation services. This suite of simulated attack services is designed to identify and exploit vulnerabilities in corporate environments.

We held an initial kickoff with IBC to meet key staff members and learn about their objectives, business operations, and overall environment. We then constructed a multi-faceted adversary simulation approach tailored to IBC's environment.

Our agreement with IBC management was that the simulated attacks would be performed without advanced notice to their team regarding the timing and methods used. This makes attack simulations more realistic. If we had telegraphed to IBS staff that a specific simulated attack was coming, they would have been on high alert, which would not be the case during a real attack.

Passive Reconnaissance

Tevora's adversary simulation testers started by conducting a two-person passive reconnaissance effort to look for ingress points for accessing IBC's facilities. Our testers—wearing business casual attire to blend in—began walking around the common, non-secured areas of the building where IBC's headquarters staff were located. They took careful note of signage, security facilities, and security staff behaviors. They also observed the behaviors of employees entering and exiting the secured areas of the building.

As part of this passive reconnaissance, Tevora's testers used their phones to capture video of the entire layout of the IBC floors, with special emphasis on entrances and exits.

By exploring the building's common areas, riding the elevators up and down, and getting out on each floor, our testers learned that:

- Badges were not required to use the elevator or access any of the floors from the elevator.
- IBC headquarters staff were primarily located on the 11th and 12th floors, where badge readers granted access to IBC working areas.
- There were no anti-tailgating systems at the entrances and exits on the IBC floors.
- Video cameras monitored IBC floor entrances and exits.

Active Reconnaissance

Our testers observed that a meeting was being held in a large conference room on the 11th floor, where vendors and IBC staff were clustered in groups talking (perhaps between meeting sessions). Badge readers granted access to the conference room, but one of our testers was able to tailgate into the room while pretending to be on the phone. After lingering in the room for ten minutes, he exited without being detected.

Our reconnaissance efforts identified the following vulnerabilities:

- No badge was required to access the building elevator or to access the IBC floors from the elevator.
- No anti-tailgating systems were used on the IBC floor entrances or exits or for accessing the large conference room.

Developing an Attack Plan

After concluding the reconnaissance efforts, Tevora's testers compared notes and reviewed the video surveillance footage they had recorded. Using this information, they crafted a plan for their simulated attack that was customized to IBC's environment.

Having developed the plan, they reminded themselves that things don't always go as expected. As Mike Tyson famously said, "Everyone has a plan 'till they get punched in the mouth." With this in mind, they discussed various contingency plans to use in the event that things didn't go as planned, which is a critical ingredient for successful adversary simulation engagements.

> As Mike Tyson famously said, "Everyone has a plan 'till they get punched in the mouth."

Initial Access

On the day of the simulated attack, both of our testers were able to enter different secure areas on the IBC floors by tailgating an IBC employee.

Having gained entry, one tester approached an IBC employee and said, "I'm with security and need to borrow your badge for a few minutes to test our system." The employee was somewhat hesitant but eventually gave his badge to the tester.

IN THIS PHASE of the simulated attack, we identified an additional vulnerability:

- Employee was not adequately trained in security.

Lateral Movement

With the badge in hand, our tester entered a restroom. After waiting a few minutes, he exited the restroom, walked down the hall, and used the badge to enter an empty work area, where he found an unattended and unlocked workstation.

IN THIS PHASE of the simulated attack, we identified another vulnerability:

• Workstation had no password protection.

Payload Installed

Attaching a pre-loaded USB drive to the workstation, our tester double-clicked an executable file on the drive that installed a payload with penetration testing tools on IBC's network. As the payload was being installed, the IBC employee that used the workstation approached and asked our tester what he was doing. The tester said he was with security and running diagnostics on the workstation. The employee asked "Am I in trouble?" Our tester responded by saying that there was no need to be concerned and that it was just a routine check that should be done in about five minutes.

Domain Admin ID Compromised

Using the installed penetration testing tools, our tester was able to compromise a domain Admin ID, which he quickly texted to his Tevora testing partner, who was in another part of the secure IBC facility. Before our first tester was able to further compromise IBC's network, he was detected and apprehended by IBC's real security team. They had had found him based on a report from the employee whose badge had been "borrowed." Having learned of our first tester's physical appearance, they had tracked him down via video surveillance camera footage.

IN THIS PHASE of the simulated attack, we identified another vulnerability:

• Administrator IDs were poorly secured.

Sensitive Accounting and Personal Information Compromised

While Tevora's first tester was being questioned by security, our second tester had tailgated into another secure area with an unattended and unlocked workstation. From this workstation, the second tester was able to use the Admin ID he'd received by text to obtain credentials for many IBC employees and use them to access a broad range of sensitive IBC accounting information and the personal information of over a hundred thousand IBC customers. After successfully compromising the IBC network, our second tester was able to leave the building undetected.

Comprehensive Reporting

Having successfully compromised IBC's network, we concluded our adversary simulation efforts and developed comprehensive documentation of our results, including physical penetration methods used, exploit code examples, and detailed remediation recommendations. We also presented a summary of our findings and recommendations to IBC management.

Positive Feedback from IBC Management

While IBC's CSO and management team were concerned about the vulnerabilities found in their environment, they were extremely pleased and impressed with the work Tevora had done, and they implemented all our remediation recommendations.

IBC remains a valued Tevora customer, and we are asked back to perform periodic adversary simulation engagements to continually probe their environment for vulnerabilities.

More Than Just a Conventional Penetration Test

In this case study, we've demonstrated how Tevora's Adversary Simulation Services go above and beyond what you would expect in a conventional penetration test by using a mix of social engineering, physical penetration, and cyberattack techniques that are highly customized for your environment. Our team of adversary simulation experts draw on their deep experience to think and act like a sophisticated real-world hacker, adapting and shifting strategies in real time as they encounter roadblocks and changes in your environment.

With a conventional penetration test, you would typically find a much less customized approach that cannot rapidly adapt to roadblocks and environmental changes. In the scenario described in this case study, it's likely that a conventional penetration testing approach would not have identified any vulnerabilities in the client environment.

Let Tevora be Your Trusted Partner

If you'd like to learn more about **Tevora's Adversary Simulation Services** or engage us to help identify and remediate vulnerabilities in your environment, just give us a call at (833) 292-1609 or email us at sales@tevora.com.