COMPASS
IT COMPLIANCE

CASE STUDY

Case Study #1 – Leveraging the Ladder

Solution Discussed: Social Engineering Assessments

Since 2010, Compass IT Compliance has partnered with organizations across the United States and beyond, helping them strengthen their information security posture. One of the solutions we offer to put your current security program to the test is onsite social engineering assessments. Through this engagement, our social engineering experts conduct research and reconnaissance on the target organization, identifying weaknesses and vulnerabilities within the access security of their physical location, such as an office building. Once recon is complete, our staff will then move to exploit flaws they've discovered. The following case study outlines an example of one of our highly successful social engineering engagements, and the vulnerabilities that our solution can help you uncover within your own organization.

Compass IT Compliance social engineering experts Jesse Roberts and Peter Fellini were assigned to conduct a social engineering assessment on two locations of a medium-sized organization. They began their assignment by conducting reconnaissance on the target organization. The two of them drove over to the locations and observed from a distance, taking note of the doors that were being used for access, operating hours, typical lunch break times, employee uniforms, and what the staff door badges looked like. They also conducted research online, utilizing sources such as LinkedIn and company "Meet the Team" pages to take note of the organization's manager names and profile pictures. These names would come in handy should anybody question their presence during the engagement.

Once recon was complete, Jesse and Peter attempted accessing the first location, which was a site that allows for customers to come in and conduct transactions inside the building. They arrived in business casual attire, like that of the staff. Peter went in first, posing as a customer, and

Jesse followed in shortly after. Once inside, Peter caused a distraction by dropping an item that caused a loud noise, which resulted in staff focusing on him while Jesse slipped behind an unlocked staff-only door. This led him to a cubicle area full of employee computers. He remained here for a short period of time before deciding to exit. On his way out he bumped into the manager of the location but was not questioned about his identity or presence. Jesse exited the employee-only area and left the building with Peter, ultimately deciding the risk of being noticed was too high due to the fact that the location had a low staff number making it more difficult to blend in and go unnoticed. The first attempt was a partial success.

The next step was to attempt gaining access to the organization's headquarters. Jesse and Peter arrived at the headquarters dressed business casual once again, like all the other staff. The two of them began by sitting outside at an employee picnic table located next to one of the entrances and drinking coffees to give the impression that they were two staff members enjoying a break. What they had found out during their recon was that this location utilized a badge system to pass the locked exterior doors, and likely further locked doors inside. Peter had noted the style and color of the badge and brought along a fake badge. Shortly after sitting at the table, they noticed an HVAC vendor exiting the building. When the door was opened, Peter timed how long it took to close and latch. When the vendor re-entered through the secure door, Jesse and Peter snuck in behind him before the door could latch without the vendor noticing. Once inside, they made their way to the employee cafeteria and continued to drink their coffee there and scope out the area. They then explored several conference rooms and a bathroom near the cafeteria. As they entered the bathroom, they passed an employee standing outside the door. Jesse asked the employee if he needed a hand with anything, to give the impression that Jesse belonged there and was a member of the organization, to which the employee stated that he was just waiting for someone in the bathroom. After exiting the bathroom, they moved further inside the building through another card-protected door, entering behind an employee who was not paying attention. Once inside this section of the building Jesse and Peter were able to access the server room, network jacks, an unlocked desktop, a list of security policies (which ironically warns employees to be aware of piggybacking through secure doors), and several other rooms. At this time, the two of them felt that staying longer would result in them being discovered, so they made the decision to exit the

building. This attempt was highly successfully in exposing security vulnerabilities within the organization.

Jesse and Peter had scheduled one more attempt at this headquarters location. They returned on a different day, now equipped with a great deal of information on the layout of the building and the security measures in place. They both now had fake employee door badges that were the same brand as the employee badges. What they had discovered was that their fake badges would cause the door lock system to flash a green light when scanned, however the doors wouldn't actually open. They entered the building in a similar fashion as the first day and made their way further inside. At one point an employee passing through a secure door looked behind her to make sure Jesse and Peter had door badges but held the door to be polite. Jesse scanned his badge anyways just to make the lock flash green and make it look like his badge was valid. Once past this door, they were able to access a cubicle area with a schedule posted that listed which staff were off that day. With this information, they selected a desk of an employee that wasn't working and browsed the cubicle. Inside the employee's desk, they found a sticky note with the employee's username and password written down. If they wished, they could've signed on to that device and wreaked havoc on the organization by installing malware or stealing data. They left this cubicle area and found a maintenance closet that allowed access to the roof, though they avoided going up to the roof in the fear that it could trigger an alarm or lock them up there. One of the final areas they wanted to investigate was the executive suite. The two of them knew the layout of this suite because the elevator had an evacuation map of the floor. They located the door to this section of the building, but the door required a badge and there was a secretary sitting just inside the entrance that would likely question their presence. To overcome this obstacle, Jesse and Peter grabbed a ladder from the maintenance closet and brought it to the executive suite door. Peter attempted to scan his card twice, which would not open the door. He knew this but wanted the secretary inside to see him attempting to use his card so she would think it was just the lock or card malfunctioning. He then tapped on the glass so she would come over to the door. She opened the door and Peter apologized and said he was from facilities and the two of them needed to fix one of the access points inside the executive suite. Peter described to her which room the access point was in, because he already knew the layout. Observing their badges, the ladder they were carrying, and the fact that Peter knew where he was going, the secretary let Peter and Jesse inside of the executive

suite. They brought the ladder into the executive board room, where they found a media center, an open network, and a laptop that could've easily been stolen. They had reached the final point inside the building that they wanted to see. As they were getting ready to leave, an employee approached them and asked who they were and what they were doing. They told him they were fixing the access point and gave a manager's name as their point of contact (which was gathered through recon beforehand). The employee hesitantly accepted this answer but began to call someone shortly after. Jesse and Peter calmly exited the building. Peter drove off in his vehicle, but Jesse was stopped by that employee in the parking lot, at which point Jesse explained who they really were and that they were contracted by the organization to conduct this assessment. He provided the relevant documents and points of contact for the engagement to assure the employee that they were not actually criminals. Though the employee successfully stopped Jesse in the very end, the engagement was still highly successfully in exposing numerous security flaws. Had the two of them been criminals, they could've inflicted serious damage on the organization's IT infrastructure and stolen valuable data in the short time they were there.

This case study is not meant to shame the organization involved, but rather expose some of the security flaws that are present within most workplaces. While it's easy to dismiss this and say that your staff would react better or your security protocols would prevent such an attempt, you do not truly know until you test your security program. Some organizations choose to administer these tests themselves. However, approaching it this way could be compared to performing your own medical exams instead of visiting your primary physician. A trained professional with decades of experience in social engineering assessments will provide a much more thorough and accurate report of vulnerabilities than a self-assessment ever could, without any issues of bias or conflict of interest. The cost of such an engagement is far less than the cost of a data breach, IT stoppage, or brand reputation damage. Contact us today to learn more about social engineering assessments and how they might benefit your organization!