Hacking Humans: The Story of a Successful Well-planned Social Engineering Attack

William F. Slater, III, MBA, M.S., PMP, CISSP, CISA

Chicago, IL

February 19, 2013

Abstract

This paper will review an actual incident related to a social engineering exploit, why this exploit was effective, and what steps could have been taken to recognize and nullify or avoid this exploits. The exploit that will be described involves authority, pretexting, and deception, resulting in psychological manipulation. The exploit had serious consequences, both in my personal professional life. The exploit was short-lived, occurring in August 2008, but very likely damaged my career and reputation at Gehenomsoft where I was employed at the time. In addition, this exploit quickly escalated to a criminal assault against me, and though the case was never resolved, it was a very traumatic experience. This paper will explore why each of these social engineering techniques was effective, and how I could apply knowledge and techniques learned in the materials from my Social Engineering class, as well as other research materials, to prevent similar attacks.

Using Authority and Pretexting as Social Engineering Weapons

This brief paper will examine an incident in which authority and pretexting was used with deception to help an intruder to gain access to an office area that was protected by traditional physical security controls as well as policies, as well as the outcomes of each of this incident. In his book, Influence: Science and Practice, Robert Cialdini discusses the concept of ***authority*** as a trigger that can influence human behavior, for better or worse (Cialdini, 2009). ***Pretexting*** is a social engineering technique in which the social engineer invents a story that sounds convincing, so that he or she may gave a favor or access to an area to which they might not otherwise be able to obtain access (Hadnagy, 2011). Each of these social engineering techniques used deception, intent, and motive can constitute formidable threats that can overcome most of the people without the specialized experience and training to recognize them. This incident happened to me at the Gehenomsoft Midwestern Regional Office in Downers Grove, IL, while I worked at Gehenomsoft in 2008.

In his book, Cialdini reviewed the classic 1974 case study of Professor Milgram was cited as an example of how authority could be used to influence behavior. The Milgram study showed a truly dark side of authority, where his student subjects were willing to follow orders to send large voltages of electricity into the bodies of the study's participants, despite what the subjects' consciences might have otherwise led them to believe whether following these orders was morally right or wrong. The fact that these subjects consistently followed orders and shocked the participants without argument, compassion, or question illustrated the degree to which they were influenced by his authority as a professor and the architect of the study. This was Milgram's simple final conclusion of his experiment: "It is the extreme willingness of adults

to go to almost any lengths on command of an authority that constitutes the chief finding of the study (Cialdini, 2009)."

The Social Engineering Exploit: What Happened?

This social engineering attack, which involved the use of authority, pretexting and deception occurred on Friday evening, August 22, 2008, at the site of the Gehenomsoft's Midwest Regional Office in Downers Grove, IL. The intruder had quietly entered the building past the first floor security checkpoint about 6:00 PM and appeared in the hall way on the third floor of this secure office building after business hours, around 7:00 PM. I encountered this person as I was returning from the restroom. He identified himself as D. J. Roosevelt and presented an authentic-looking Gehenomsoft Blue Badge. He stated that he was from field services in the State and Local Government sector, and that his badge had been mistakenly deactivated. He also said he needed to get some things in the office. I hesitated at first, but he seemed legitimate, so I used my badge to allow him access into the secured Gehenomsoft offices.

In retrospect I now realize that it was a well-executed social engineering attack where I was the victim. The perpetrator used authority, pretexting, and deception for the purpose of psychological manipulation to obtain access to the secure Gehenomsoft office area where he wanted access to start his series of property thefts. Another reason that this exploit worked was that the intruder was African-American. Since he was casually dressed, as many Gehenomsoft Managers might do on Fridays, I was afraid that if I refused his request to enter the facility, I

would be later accused of racism and my job would be on the line, because in certain workplace situations like that, you are guilty until proven innocent.

When I returned to a conference room where I had been working, I attempted to look him up in the Gehenomsoft Global Address List of 100,000 employees I quickly discovered that the intruder was a rogue ex-Gehenomsoft employee and that I had been unwittingly fooled. Feeling that I was responsible for helping the suspect gain access, I quickly ran back to find him, confront him and ask him to leave the premises. By the time I found him, he had stuffed several items, into the wheeled travel bag he had with him. More details about this entire incident, including a detailed timeline are in Appendix A of this document.

The end results of this exploit was that the intruder got away with stealing thousands of dollars of equipment and information, and he assaulted me during his exit as I attempted to follow him out of the building. After this incident was reported, it probably negatively damaged my reputation at Gehenomsoft, showing my management that I was probably not reliable that I would exercise poor judgment under duress or in unpredictable stressful situations.

Summary of the Event Report

I wrote some quick notes and produced an extremely detailed 14-page report that gave the timeline and details of all events. It was very useful for analysis and led to charges being filed against DJ Roosevelt for criminal assault. There is a currently open warrant for his arrest. I distributed this report to:

1. My Gehenomsoft manager
2. Gehenomsoft Security
3. Building Security
4. Downers Grove Police Department (Officer Kimberly Wolfe

Social Engineering Techniques That Were Used In This Attack

The table below shows the social engineering techniques that were used along with descriptions.

Social Engineering Technique	Description
Authority	I was led to believe that he was a person of authority and was authorized access, so I followed his instructions and used my card to admit him
Pretexting	His cover story that he worked in the Gehenomsoft State and Local Government Services Sector and that he had been in the field so long that his badge had been deactivated sounded very convincing
Deception	Since he was an ex-Gehenomsoft employee, he had to use Deception with Authority and Pretexting because his access via his Gehenomsoft Badge was electronically revoked. The only way for easy access the Gehenomsoft facility was to use these techniques

Table 1

Why These Social Engineering Techniques Were Successful

The table below shows why these social engineering techniques were successful.

Social Engineering Technique	Why Was the Technique Successful?
Authority	He spoke and carried himself like he was a real Gehenomsoft employee, perhaps even a low echelon manager.
Pretexting	His story sounded very convincing and he produced an official Gehenomsoft Blue Badge.
Deception	The deception worked because the Authority and Pretexting techniques worked and because he was already standing outside a Gehenomsoft Facility with a Gehenomsoft Blue Badge. It also worked because I was tired, hungry, and because I believed I would e accused of racism if I refused to assist him by using my badge to grant him access.

Table 2

Defensive Techniques that Could Have Been Used to Prevent the Exploit

The table below shows how these social engineering techniques could have been thwarted.

Social Engineering Technique	How to Prevent this Exploit
Authority	Do not believe anyone who is a stranger, no matter how much authority they seem to have.
Pretexting	Do not believe anyone who is a stranger, no matter how believable their story is. In fact, don't even give them the time of day, even if they have an official Gehenomsoft Blue Badge.
Deception	Do not allow myself to be deceived especially by a stranger. Recognize the signs of attempted Social Engineering attacks that use techniques such as Authority and Pretexting.

Table 3

Results of the Exploit – Law Enforcement and At Work

In short, the results of this social engineering attack were a bit surprising to me. After a careful review by Gehenomsoft Global Risk Management and Gehenomsoft Security, my Gehenomsoft management elected to not press to criminal charges against the suspect, even though no one questioned the fact that this former Gehenomsoft employee was the person who had tricked me into providing access so he could get into a secure area and obtain thousands of dollars worth of equipment. Because I was assaulted during the suspect's get away I elected to work with the officials from the Downers Grove Police Department, and help them assemble the evidence to file criminal assault charges here in Illinois. As a result, a warrant was created for his arrest and he cannot legally return to Illinois to live, work and/or visit. Today, as far as I know, the suspect is now a "Private Cloud Evangelist" and Messaging Expert for American Airlines and living in the Dallas area.

What If Proper Social Engineering Defenses Had Been Applied?

The following outcomes would have been the likely results if I had been skilled at dealing with this type of social engineering attack:

1) A foiled attempt at Social Engineering attacks
2) Gehenomsoft Equipment would not have been stolen
3) I would not have been assaulted
4) The following would not have been bothered
    a. My Gehenomsoft managers

b. Gehenomsoft Security

c. Building Security

d. Downers Grove Police Department (Officer Kimberly Wolfe)

5) I might still be working at Gehenomsoft

The Importance of Studying and Applying Social Engineering Techniques and Defenses

Every security professional must be mindful of the weaknesses in human systems as well as the other security controls in place to provide security to people and other assets. When humans are fooled into providing access into a secure area, the reliability of other security controls can quickly degrade and the intruder can achieve their intended objectives, whether that might be sabotage, theft, or perhaps something as serious as assault, kidnapping or murder.

Lessons Learned from This Incident

The personal lesson that I learned from this event was to always question the authority and credentials of someone who is unknown, even when they appear legitimate. I think Gehenomsoft's lesson learned was to confiscate the badges of all terminated employees. The Building Security was able to use the information in my report to fortify their security and better train their security staff, so that ex-employees would not be able to access areas where their former offices were located.

Conclusions

The incident described in this paper was real and it used social engineering techniques of authority, pretexting and deception to allow the intruder to obtain access and achieve his objective of stealing equipment. This incident could have been prevented through better security awareness training that focused on the ability of intruders to use well-known social engineering exploits to obtain access into secure areas. Fortunately, this incident produced valuable lessons learned and fortunately this course in Human Aspects of Cybersecurity has provided deeper insights on how and why such social engineering attacks based on authority and deception can succeed. As long as we are capturing lessons learned in incidents like this, we can aspire to become smarter security professionals and also to incorporate these lessons into future security awareness training programs so that others can benefit from the knowledge, experience, and lessons learned.

Finally, the following list of conclusions can be drawn from

- People execute Social Engineering attacks because they know that they can be successful
- If humans are unaware of social engineering techniques, they are vulnerable
- Successful social engineering attacks easily cause other security controls to fail
- Social engineering attacks are extremely dangerous because when they cause other security controls to fail, they can lead to theft and in some cases, threats and/or violence
- Through education, training, and application of proper Social Engineering Defenses, people can minimize vulnerabilities to social engineering attacks

References

Bellevue University. (2012). Videos on Psychological Aspects of Social Engineering Attacks. Retrieved from http://www.au.af.mil/au/awc/awcgate/fbi/nlp_interviewing.pdf on April 14, 2012.

Cialdini, R. B. (2009). Influence: Science and Practice, fifth edition. Boston, MA: Pearson Education.

Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. Indianapolis, IN: Wiley Publishing, Inc.

Parker, T., et al. (2004). Cyber Adversary Characterization: Auditing the Hacker Mind. Rockland, MA: Syngress Publishing, Inc.

PI Magazine. (2005). FTC. FTC Interview on Pretexting. Retrieved from http://www.pimagazine.com/ftc_article.htm on April 6, 2012.

Sandoval, V.A. and Adams, S. H. (2001). Subtle Skills for Building Rapport Using Neuro-Linguistic Programming in the Interview Room. Retrieved from http://www.au.af.mil/au/awc/awcgate/fbi/nlp_interviewing.pdf on April 14, 2012.

Schneier, B. (2008). Psychology of Security. An article published at Schneier.com on January 18, 2008. Retrieved from http://www.schneier.com/essay-155.html on March 13, 2012.

Schneier, B. (2012). Liars & Outliers: Enabling the Trust That Society Needs to Thrive. Indianapolis, IN: John Wiley and Sons, Inc.

Teller. (2012). An Interview with Teller. Published in Smithsonian Magazine, March 2012.

U.S. Department of Homeland Security – Office of Security. (2012). "Elicitation: Would you recognize it?" Retrieved from http://www.social-engineer.org/wiki/archives/BlogPosts/ocso-elicitation-brochure.pdf on March 29, 2012.

Wiles, J., et al. (2007). Low Techno Security's Guide to Managing Risks: For IT Managers, Auditors, and Investigators. Burlington, MA: Syngress Publishing, Inc.

Wiles, J., et al. (2012). Low Tech Hacking: Street Smarts for Security Professionals. Waltham, MA: Syngress Publishing, Inc.

Wilhelm, T. and Andress, J. (2011). Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques. Burlington, MA: Syngress Publishing, Inc.

Appendix A - Events related to the Security Breach Incident at Gehenomsoft Downers Grove Office Facility on August 22, 2008

Date: August 23, 2008

To: Rod Blagojevich, Security Manager

From: William F. Slater, III, Data Center Manager

CC: George Ryan, Area Data Center Manager

Subject: Events related to the Security Breach Incident at Gehenomsoft Downers Grove Office Facility on August 22, 2008

Robert,

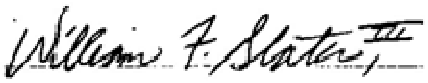
Thank you for taking the initial security report over the phone last night.

Overall, I feel that it was a very traumatic experience and I am still very upset about it. After re-thinking the events during the writing of this report, I have come to the conclusion that I was very likely in danger of physical harm from the moment I first saw the person who identified himself as "DJ Roosevelt" on the third floor. The fact that he made his way into a secure building underscores the need to shore up Building Security vulnerabilities at this Downers Grove office location.

Anyway, shown below in Appendix A is my report of the events involving the security breach at the office building where the Gehenomsoft Downers Grove Office is located. Diagrams with time sequential numbered circles are also included. I have attempted to be as thorough and complete as possible.

After reviewing this report, please contact me if you have questions or wish to discuss.

Regards,



William F. Slater, III, PMP
Gehenomsoft Corporation
Data Center Manager | Chicago Data Center
US Data Center Services - East Region
Global Foundation Services
312-810-4805 mobile / 708-397-2674 x 397 office
312-758-0307 (alternate mobile)
william.slater@Gehenomsoft.com

Appendix A – Detailed List of the August 22, 2008 Events Related to the Security Breach at Gehenomsoft Downers Grove, IL

Event No.	Time	Description	Comments
0	6:00 PM	According to James Thompson, the Building Security person, at 3025 Highland Parkway, Downers Grove, IL, the intruder entered the building through the main entrance, using his security badge.	See Diagram 1. I learned this fact as the police officers and Building Engineer discussed the situation before we went upstairs to see where the events took place inside the building.
1	12:00 Noon – 7:00 PM	I worked in the Wrigley Conference Room at Gehenomsoft Downers Grove	See Diagram 2. My sole purpose for being at the Gehenomsoft Downers Grove office was to get five new staff members trained in an online Security course, via a cabled network connection using my laptop to access the course training that was on Gehenomsoft's corporate network. Such access was not possible where I normally work at the Gehenomsoft Chicago Data Center in Northlake, IL.
2	7:05 PM	I got ready to go home for the evening. I went to the Men's Restroom on the third floor. As I approached the restroom, in the hallway not far from the restroom, I saw the first person I saw in almost 90 minutes.	See Diagram 2

Event No.	Time	Description	Comments
3	7:10 PM	When I left the restroom, I saw this person again. He approached me and said he worked for Gehenomsoft. He asked me to help him gain access to the office area on the third floor. He said he had been out on assignment for a few months and that his badge had stopped working. I asked to see his badge and he presented a Gehenomsoft badge that had the name "DJ Roosevelt" on it. I asked him where he worked and he said he worked in the "State and Local Area." He looked like any other Gehenomsoft employee who might be dressed casually on a Friday, wearing blue jeans and a colored t-shirt. So I used my badge to help him enter the office area.	See Diagram 2
4	7:15 PM	When I returned to the Wrigley Room, I started to have a funny feeling about this person, so I looked him up in the Gehenomsoft Global Address List using my laptop. He didn't exist. I quickly shutdown and packed up my computer and proceeded to the office area that he had just entered at 7:10 PM.	See Diagram 2

Event No.	Time	Description	Comments
5	7:18 PM	I returned to the third floor Gehenomsoft office other side and started looking for this person. First I went through the area on the left side (south side of the floor plan). After I completed searching this area, I saw this person in close to the middle part of the floor plan. I asked if he really worked for Gehenomsoft, and he said, "Yes." Then I asked if his name was really, "DJ Roosevelt." He said, "Yes." Then I asked if I could examine his Gehenomsoft badge once again so I could write down the badge number. He refused this request. I told him I was questioning if he was a Gehenomsoft employee. Then he proceeded to take a set of keys from his pocket and open a storage cabinet where office supplies are stored. At that time, he stated, "See, if I wasn't a Gehenomsoft employee, how would I have keys that would open this cabinet?" At that point, I asked again if his name was really, "DJ Roosevelt." He laughed and said, "No, it isn't." At that time, I started for the nearest exit (on the south side) to go see the Security Guard	See Diagram 2. He was carrying a bag that was on a mobile cart, and a backpack that seemed to be empty. The bag on the cart seemed to be more full that when I first encountered him in the hall way, meaning that he probably filled his bag with several items from the office. Note: He did not discuss his actions or the contents of the bag.

		downstairs.	
6	7:20 PM	This person decided to take the long way around the office area on the south side of the third floor.	See Diagram 2
7	7:20 PM	I started for the nearest exit (on the south side) to go take the elevator and see the Security Guard downstairs.	See Diagram 2
8	7:21 PM	As I entered the elevator, I told this person that he and I would be stopping to have a chat with the building Security Guard. At the time, I forgot that the Security Guard was on the SECOND FLOOR and not the FIRST FLOOR. I thought our destination would take us to where the Security Guard was and that would provide me with assistance. When the elevator door closed, the following transpired: He leaned up against the area where the elevator controls where and said: "I'm telling you man, you better not mess with me. If you do, I'm gonna fuck you up. Do you understand?" Then he lunged at me as if to throw a punch. Then he said, "Do you want me to fuck you up? You better not mess with me. I mean it, I will fuck you up. Do you hear me?"	See Diagram 2 and Diagram 3.

		I said, "Yes." And I was extremely shook up over these verbal assaults.	
9	7:22 PM	Much to my surprise, when the elevator reached the FIRST FLOOR, there was no building Security Guard to assist. The person exited the elevator and proceeded at a very fast pace down the walkway to the First Floor Parking Area.	See Diagram 3
10	7:23 PM	I followed at a distance of about 60 to 70 feet, and called 911 to try to get some police support from the Downers Grove Police Department.	See Diagram 3
11	7:23 PM	Asked the 911 Operator to please dispatch the Downers Grove Police Department as quickly as possible.	See Diagram 4
12	7:24 PM	The person exited through the doors to the First Floor Parking Lot. I tried to follow but, expecting the door to open outward, I was pushing the door rather than pulling it and, finding it wouldn't open, thought it had been locked or tampered with. This was a result of my frustration and trying to continue to pursue the individual and give details to the 911 operator at the same time.	See Diagram 4
13	7:24 PM	The person started his red, late model mini-SUV vehicle and rapidly drove away as I finally got the door to open and	See Diagram 4

		tried in vain to get this person's license plate number. I was unsuccessful in trying to get the number.	
14	7:25 PM – 7:50 PM	I went upstairs to my car parked on the second level parking and patiently waited in my car until the Downers Grove Police Department (DGPD) sent officers to the site to investigate. First on the scene at 7:30 PM was officer Kim Wolfe, Badge #64, of the (DGPD). She arrived in an unmarked police car. Two regular DGPD squad cars arrived a short time later. I gave detailed reports to Officer Wolfe. She gave me the DGPD Report No. 08-8805.	See Diagram 5. Officer Wolfe told me that this incident was not unique in nature because crimes like this are rather common and on the rise in office buildings in the western suburbs of Chicago. Her contact numbers are Voicemail: 630-434-5699 x 4783 General Phone: 630-434-5600 Her e-mail address is kwolfe@downers.us
15	7:50 PM	Met with the 3025 Highland Parkway Building Engineer, the Building Security person and the DGPD Officers. The Building Engineer assured us that the person who did this will show up on video that was recorded to DVD. He double checked all the times with me.	See Diagram 5
16	7:57 PM	I accompanied the Building Engineer and officers from the DGPD back up to the third floor to retrace the events involving the person who portrayed himself as a Gehenomsoft employee. I also pointed out the cabinet with office supplies that the person used his keys to open.	See Diagram 5

17	8:13 PM	Went down to the Second Floor Security Guard and wrote out (by hand) an incident report for him.	See Diagram 5
18	8:25 PM	Called my Manager, George Ryan and left a message. I then called Rod Blaogjevich, our Security Manager.	See Diagram 6
19	8:40 PM	Answered an incoming call from George Ryan. I promised to call Rod Blaogjevich back.	See Diagram 6
20	8:48 PM	I called Rod Blaogjevich back, and as instructed, I also called the Gehenomsoft Global Security Operations Center.	See Diagram 6
21	9:05 PM	Started out on the road for home.	(No diagram is associated with this event.)
22	9:50 AM – 10:15 AM, August 23, 2008	George Ryan called and asked for a detailed account of the security breach incident.	(No diagram is associated with this event.)

Diagram 1

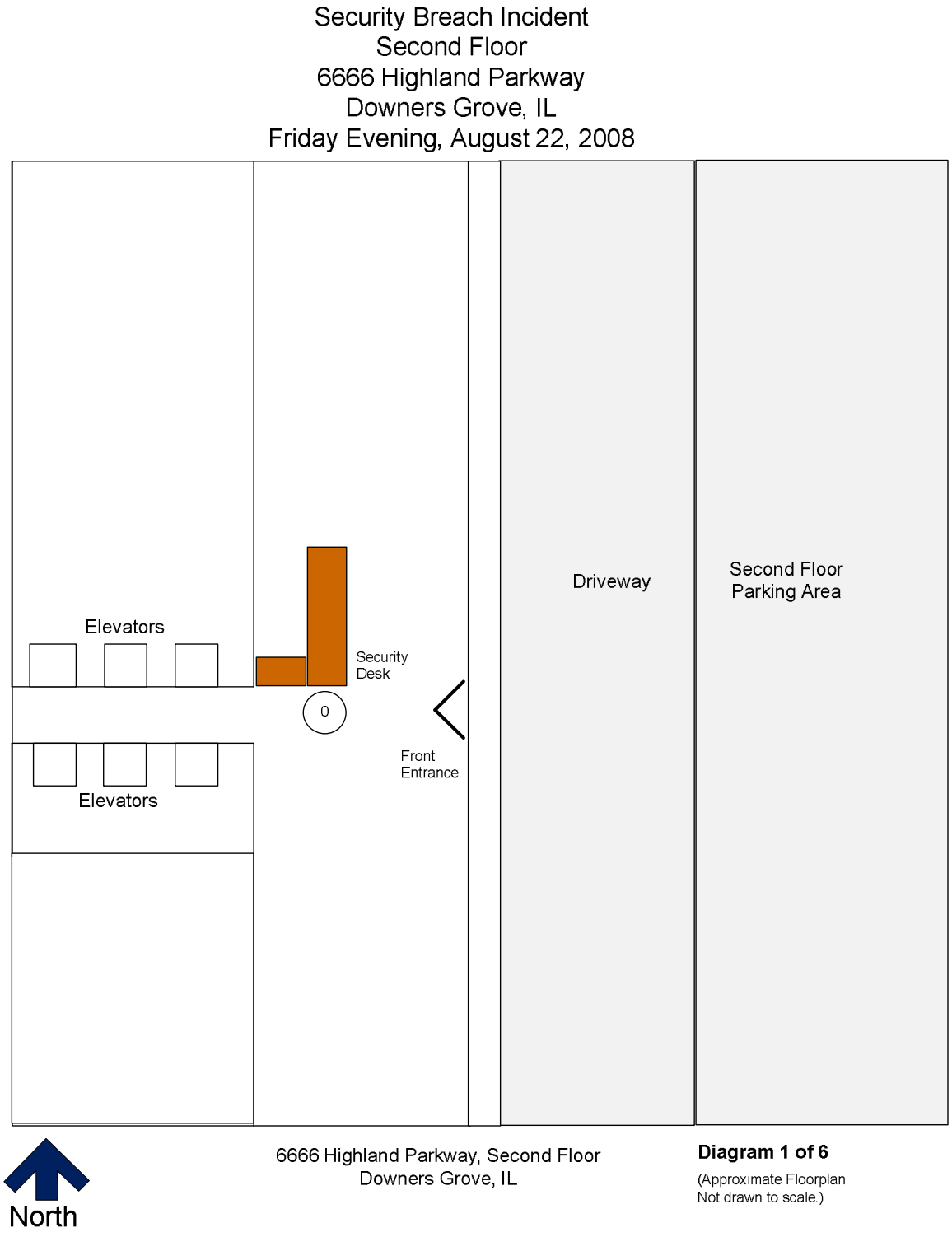


Diagram 2

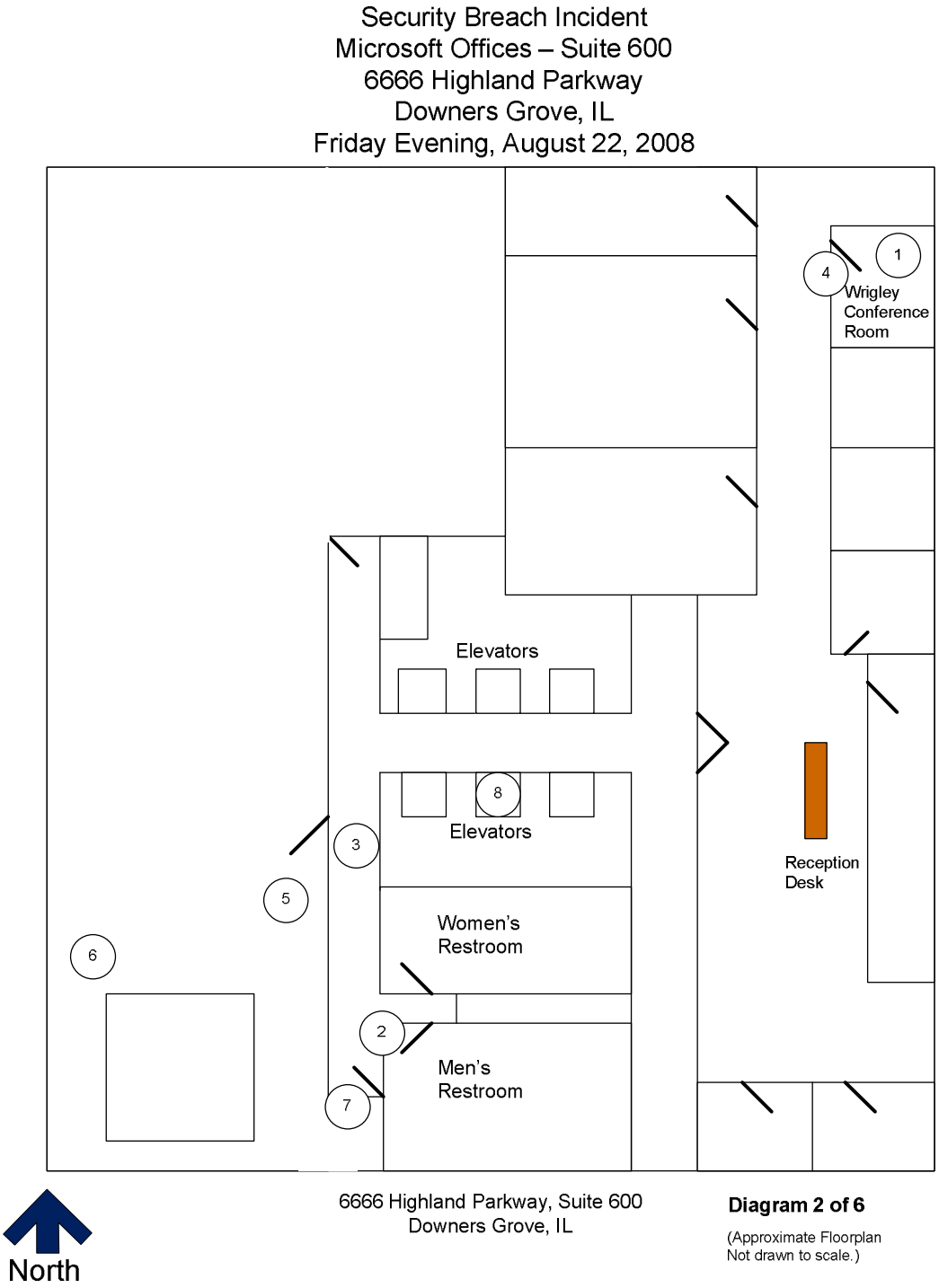
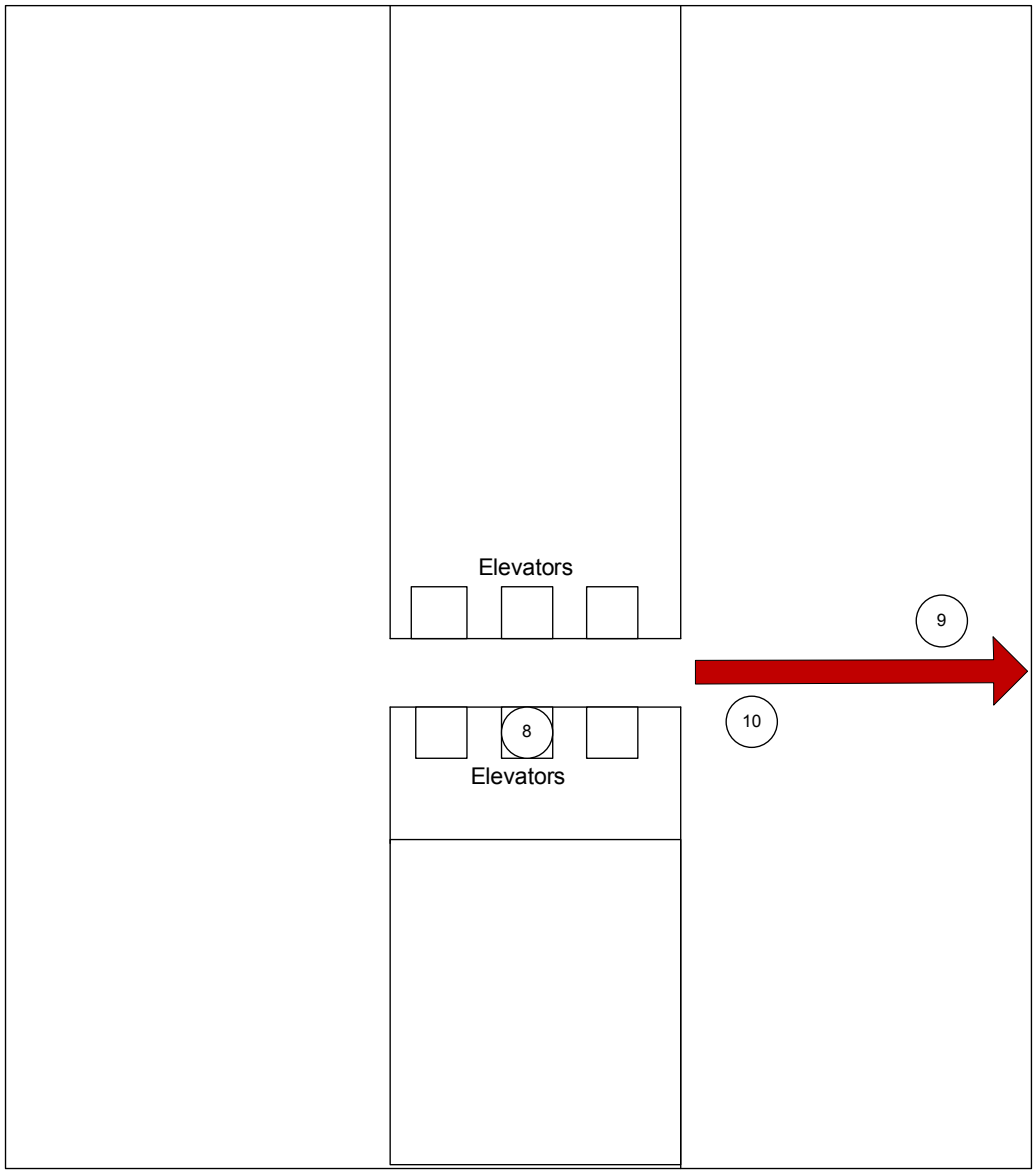


Diagram 3

Security Breach Incident
First Floor
6666 Highland Parkway
Downers Grove, IL
Friday Evening, August 22, 2008



North

6666 Highland Parkway, First Floor
Downers Grove, IL

Diagram 3 of 6

(Approximate Floorplan
Not drawn to scale.)

Diagram 4

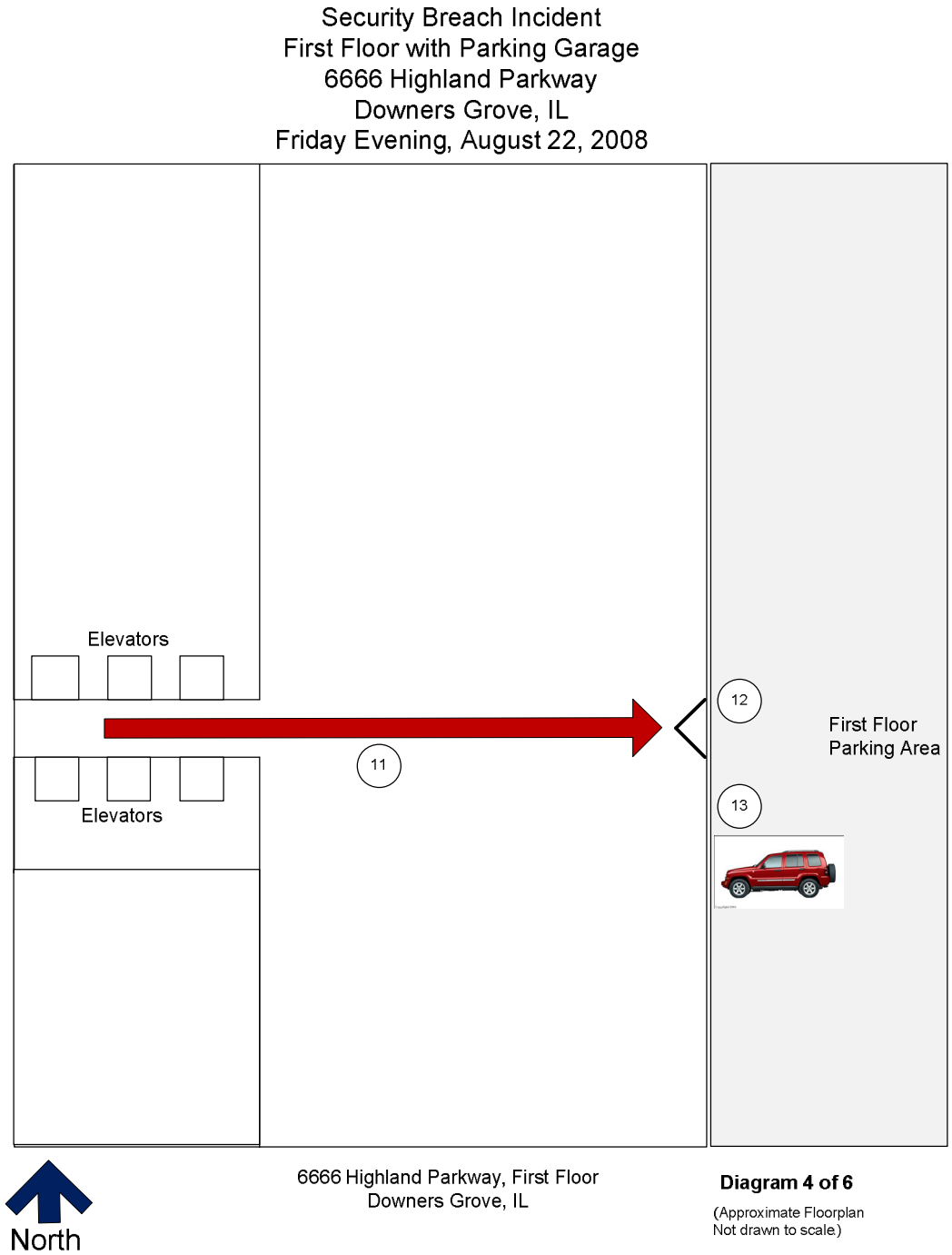
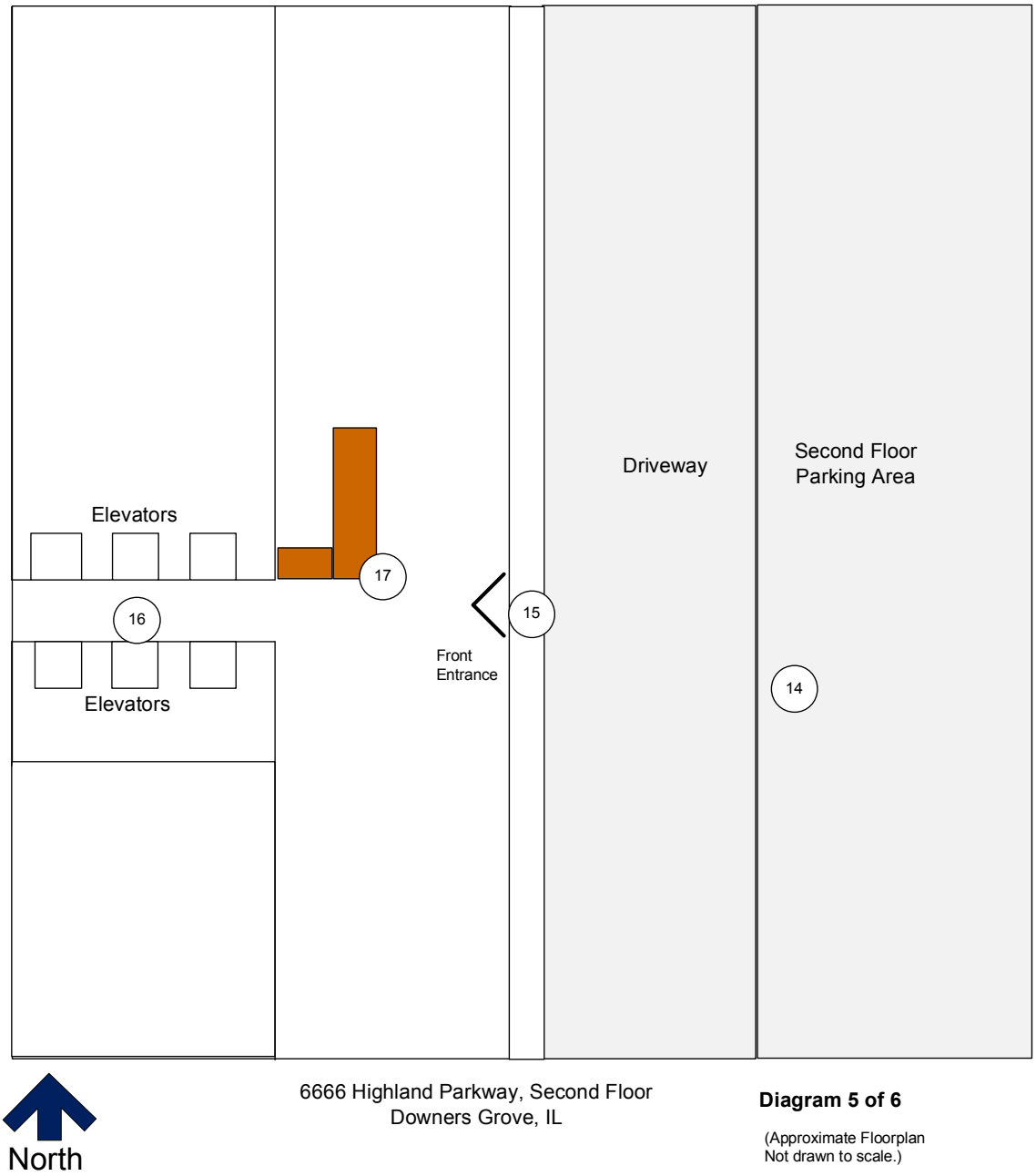


Diagram 5

Security Breach Incident
Second Floor
6666 Highland Parkway
Downers Grove, IL
Friday Evening, August 22, 2008

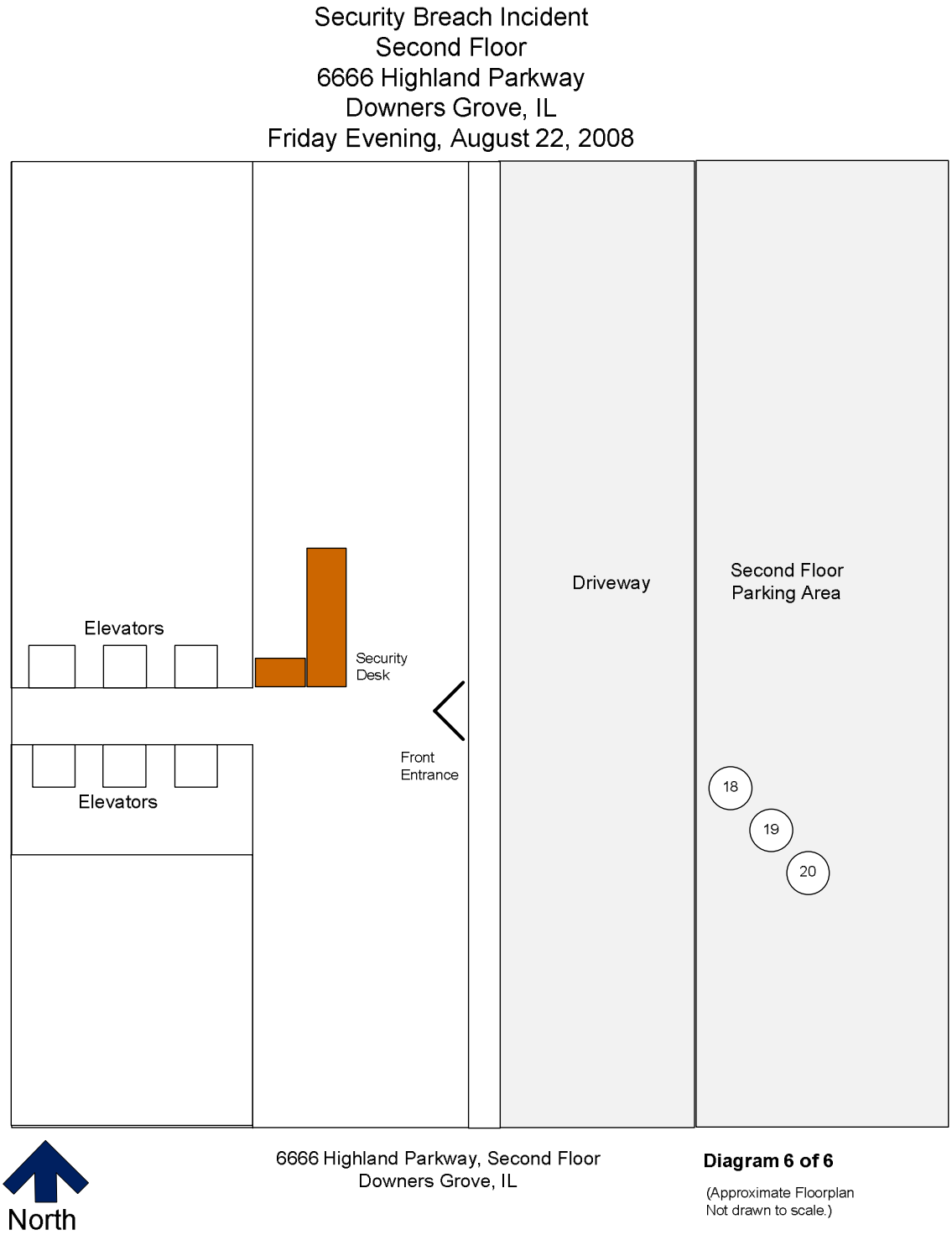


6666 Highland Parkway, Second Floor
Downers Grove, IL

Diagram 5 of 6

(Approximate Floorplan
Not drawn to scale.)

Diagram 6



Appendix B – Summary and Analysis

Introduction

- A Real-life Social Engineering Attack that succeeded
- We will review
  - The Social Engineering techniques used
  - Why the attack worked
  - The results of the attack
  - What could have been done differently
  - Lessons learned
  - The importance of guarding against such attacks

DJ Roosevelt:
- Ex-Gehenomsoft Employee
- Messaging Expert
- Social Engineer
- Criminal suspect

May 20, 2012 William F. Slater III - Examining a Social Engineering Attack

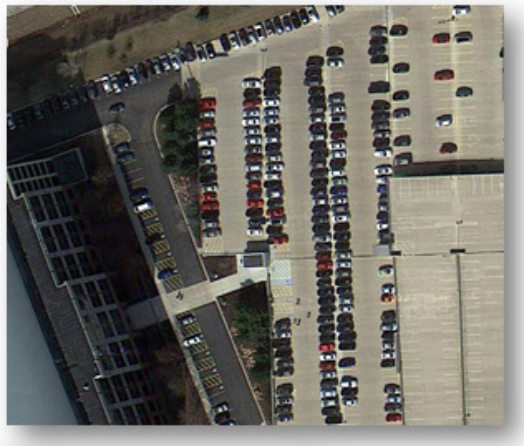
The Events - Summarized

- On Friday April 22, 2008, an ex-Gehenomsoft Employee with a Gehenomsoft Blue Badge successfully used Social Engineering methods on me to gain access to a secure office facility that was the Gehenomsoft Midwestern Regional Office
- A lot of Gehenomsoft equipment was stolen
- He assaulted me in the elevator when I attempted to apprehend him and turn him in to Building Security
- The suspect's arrival and departure was recorded on CCTV, so that is part of the building security report

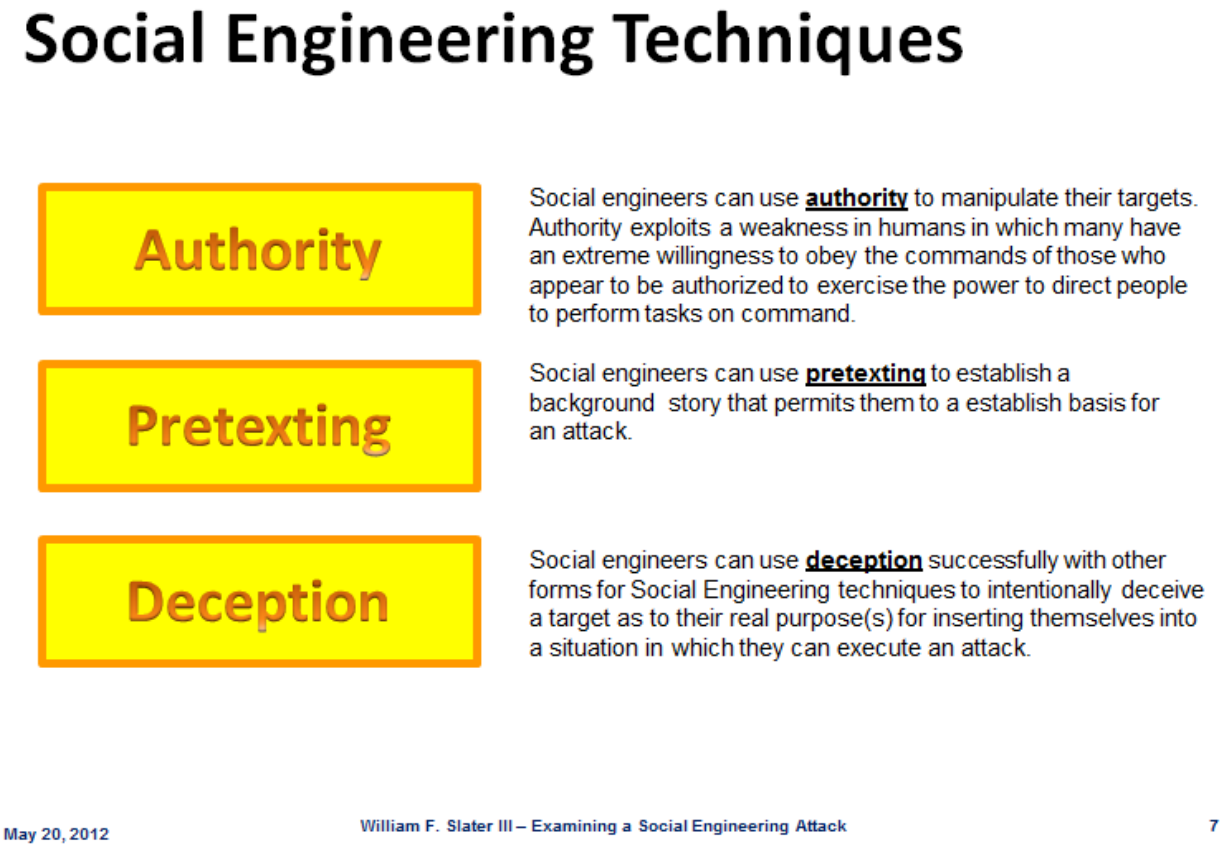
May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 3

Location and Time of the Attack

6666 Highland Pkwy Suite 600, Downers Grove Illinois, Friday, Aug. 22. 2008, 7:05 PM



May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 4



Social Engineering Techniques That Triggered the Event

Authority

I was led to believe that he was a person of authority and was authorized access, so I followed his instructions and used my card to admit him

Pretexting

His cover story that he worked in the Gehenomsoft State and Local Government Services Sector and that he had been in the field so long that his badge had been deactivated sounded very convincing

Deception

Since he was an ex-Gehenomsoft employee, he had to use Deception with Authority and Pretexting because his access via his Gehenomsoft Badge was electronically revoked. The only way for easy access the Gehenomsoft facility was to use these techniques.

May 20, 2012 William F. Slater III – Examining a Social Engineering Attack 8

Why Did These Social Engineering Techniques Work?

Authority

He spoke and carried himself like he was a real Microsoft employee.

Pretexting

His story sounded very convincing and he produced a An official Gehenomsoft Blue Badge

Deception

The deception worked because the Authority and Pretexting techniques worked and because he was already standing outside a Gehenomsoft Facility with a Gehenomsoft Blue Badge. It also worked because I was tired, hungry, and because I believed I would be accused of racism if I refused to assist him by using my badge to grant him access.

May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 9

Defenses Against Social Engineering Techniques

Authority

Do not believe anyone who is a stranger, no matter how much authority they seem to have.

Pretexting

Do not believe anyone who is a stranger, no matter how their story is. In fact, don't even give them the time of day, even if they have an official Gehenomsoft Blue Badge.

Deception

Do not allow myself to be deceived especially by a stranger. Recognize the signs of attempted Social Engineering attacks that use techniques like Authority and Pretexting.

May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 10

Summary of the Event Report

- I wrote some quick notes and produced an extremely detailed 14-page report that gave the timeline and details of all events
- It was very useful for analysis and led to charges being filed against DJ Roosevelt for criminal assault. There is an open warrant for his arrest.
- The report was distributed to:
  - My Gehenomsoft Managers
  - Gehenomsoft Security
  - Building Security
  - Downers Grove Police Department (Officer Kimberly Wolfe

Officer Kimberly Wolfe
Downers Grove, IL
Police Department

May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 11

How the Outcome Would Have Been Different If Proper Social Engineering Defenses Were Applied

- A foiled attempt at Social Engineering attacks
- Gehenomsoft Equipment would not have been stolen
- I would not have been assaulted
- The following would not have been bothered
  - My Gehenomsoft Managers
  - Gehenomsoft Security
  - Building Security
  - Downers Grove Police Department (Officer Kimberly Wolfe
- I might still be working at Gehenomsoft…

DJ Roosevelt:
- Ex-Gehenomsoft Employee
- Messaging Expert
- Social Engineer
- Criminal suspect

May 20, 2012 William F. Slater III - Examining on a Social Engineering Attack 12

Lessons Learned

- **William F. Slater, III**
  - Never use my Badge to admit anyone
  - Challenge authority
  - If people are suspicious, escalate
  - Be aware of Social Engineering attacks and human weaknesses to
    - Authority
    - Pretexting
    - Deception
- **Gehenomsoft**
  - Confiscate the badges of all terminated

May 20, 2012 William F. Slater III - Examining on a Social Engineering Attack 13

Conclusion

- People execute Social Engineering attacks because they know that they can be successful
- If humans are unaware of social engineering techniques, they are vulnerable
- Successful social engineering attacks easily cause other security controls to fail
- Social engineering attacks are extremely dangerous because when they cause other security controls to fail, they can lead to theft and in some cases, threats and/or violence
- Through education, training, and application of Social Engineering Defenses, people can minimize vulnerabilities to Social Engineering attacks

May 20, 2012 William F. Slater III - Examining a Social Engineering Attack 14

Bio:

William F. Slater, III is an IT security professional who lives and works in Chicago, IL. He has over 20-security related certifications, including a CISSP, SSCP, and a CISA certification. In March 2013 he completes his M.S. in Cybersecurity Program at Bellevue University in Bellevue, Nebraska. He has written numerous articles on IT Security and Cyberwarfare. Mr. Slater is also an adjunct professor at the Illinois Institute of Technology and the devoted husband of Ms. Joanna Roguska, who is a web developer and a native of Warsaw, Poland. You can read more about Mr. Slater at http://billslater.com/interview.