Global Information Assurance Certification Paper

Breaking the Piggy Bank Open from the Inside Out

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 - Case Study in the Effectiveness of a Physical Security Attack to Bypass Perimeter Network Defenses

Submitted by: Matthew T. Davis
Location: Cleveland, Ohio

Paper Abstract: The Greeks have shown us with the Trojan Horse that even the strongest perimeter can be breached via an effective physical attack involving social engineering. As more organizations beef up their network defense perimeter, it may all be circumvented if proper physical controls and user awareness are not in place. This paper is a case study of a Midwestern bank that requested to have its physical security assessed via penetration testing including secondary information gathering and testing the resulting vulnerabilities found.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

List of Figures

Abstract/Summary

Perhaps one of the most enduring and legendary examples of a physical security breach that resulted in a devastating blow is the Greek army's use of the Trojan Horse to compromise the city of Troy. In IT security, a Trojan Horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage"[1]. Though this is a very typical problem, the focus of this paper is to understand the problem illustrated by the original Trojan Horse – how a lapse in physical security controls can circumvent good technical perimeter controls.

In both Homer's *Iliad* [2]and Virgil's *Aeneid* [3], we are presented with a story in which the Greeks are seeking to free Helen, the most beautiful woman in the world and one of their queens who had been kidnapped by the Trojan prince Paris. After roughly 10 years in to the siege of Troy, the Greeks had surrounded the city, but were growing weary of the war and missing their families. Athena, the goddess of way, gave Odysseus the idea to build the Trojan Horse to gain entry to the city. Today, malicious attackers can also get frustrated in long-drawn out attempts to run slow attacks to evade Intrusion Detection Systems (IDS) and defeat firewall and systems controls.

The Greeks executed a very intricate plan in order to get the Trojan Horse into the city. After building the Horse and putting soldiers inside, the Greeks burned their camps and put up the sails on their ships to appear to give up and leave. Additionally, a Greek spy named Sinon was left behind who, upon the Trojans finding the Horse, convinced them he had been deserted and the Horse would bring them luck. Despite the objections from the high priest of Troy, Laocoon, and his daughter, Cassandra, the Trojan Horse was brought into the city. Today, the art of social engineering can be used to prey upon the inherit trust in human behavior despite warnings conveyed through awareness training and in security policies.

The final blow to the city of Troy occurred in the middle of the night. The entire city, relieved to be rid of the Greeks, threw a massive feast and partied well into the night until passing out. Then Sinon signaled the Greek army and released Odysseus and the other Greek soldiers, who proceeded to kill the gate guards and let the Greek army into the city. Today, it is not uncommon to find an organization with good external controls, but lacking good internal controls on the 'trusted' network. And with the advent of wireless technology, it is not difficult to gain (and regain) entry into a targeted network once physical access has been obtained, especially with the help of a malicious internal user.

The following case study involves a Midwestern bank that my company had done previous external attack and penetration activities include the areas of war-

dialing, Internet/firewall review and web application security. The scope of this new project was to assess the banks physical security controls in a covert manner and report on what the impact was to the internal network security. A second portion of the project involved overt activities assessing the internal network security of key servers. The study outlines how some of problems the Trojans faced are pertinent to all organizations in today's IT security world.

Before

The bank has a very typical setup. There is a main branch which houses most of the banks resources including network servers and services, corporate staffing, and the main vault as well as customer facing operations. The branch offices function as retail locations for customer services and have WAN connections back to the main branch and local resources to support day-to-day operations.

From the previous engagement, my company was well-aware of the banks IT perimeter controls which include a firewall with intrusion detecting and intrusion prevention abilities. These abilities included standard IDS/IPS threshold monitoring for ping sweeps and port scans as well as event specific monitoring for signature-based attacks like buffer overflows. Additionally, as a result of the previous assessment, additional system hardening was done. Therefore, the bank's network perimeter controls were very effective and would be very hard to compromise.

The new engagement was to focus on the main branches physical security, though remote branches were also assessed. As a proof-of-concept, the rules of the engagement allowed our firm to show what information could be gathered as a result of any breach in physical security. This bank had implemented a mix of physical security controls including key locks, button locks, proximity badge readers with zones, and biometric readers for the data centers – though this information was not shared with my company ahead of time. We were informed that the bank was two stories with a basement and that the vault was off-limits and not part of the scope. Additionally, no destructive means were to be used e.g. a crowbar or breaking glass.

The timeline of this engagement started with arrival on a Sunday evening. The initial covert phase's main goal was to breach physical security on Monday as well as Tuesday to show repeatability. The overt phase was conducted on Wednesday and Thursday and the results were used to further identify any additional risks that could result with more time. My company used a team of 3 members, including myself, chosen for their social engineering skills, network penetration skills, and physical security skills. As a precautionary measure, each member of the team was provided a 'get out of jail free' letter from the bank including key bank contacts as well as our purpose.

Current Security Posture

Until now, the bank had not discovered any breaches in physical security, but was aware of possible areas that might be weak. These areas were not discussed with my company at the beginning of the engagement. Though the bank had done some of its own assessments, it had not been formally reviewed by an independent third-party.

The Path of Least Resistance

As with most organizations, though strong network perimeter controls may be in place, the internal network is much more susceptible to attacks. This is largely due to the philosophy that is more important to guard against attacks originating from the Internet as noted in a 2004 Global Information Security Survey, "many respondents appeared fixated on external threats such as viruses, the more likely and most lethal threats are those originating from within an organization's growing extended enterprise"[4].

Therefore, many organizations have spent a great deal of resources putting very good network perimeter controls in place. These controls make it extremely difficult and time consuming for someone to gain access to the bank from the Internet. Due to their financial assets, banks are often a prime target for an attack. A determined attacker will often take the path of least resistance and look for other ways to gain access to the organization's network.

As a result of focusing on the network perimeter, physical controls may be overlooked. Banks, however, are typically very well aware of how to implement physical security. But with many facilities having personnel inside the building 24x7, most banks focus most of their physical controls around the vault. This includes their alarm systems. So, facility access controls may not be strong enough to stand an attack.

And finally, even strong physical access controls can be breached through a good social engineering attack. And though end-user security awareness training is the best defense, it's not always practiced so much as it's preached. As noted from the above survey, respondents "named 'lack of security awareness by users' as the top obstacle to effective information security, however, only 28% listed 'raising employee information security training or awareness' as being a top initiative in 2004."[5]

Access to the Network

There are some obvious risks that arise from just the physical access itself. An intruder can usually find customer information for example as account numbers

and balances. Another physical risk, that can have impact in a network attack, includes access to personnel desks - which oftentimes may contain papers with systems information, usernames and passwords, keys and badges, and even personal information that could be used in a social engineering attack.

From a technical risk, most risks originate from the ability to access the network infrastructure. This includes installing keystroke loggers, using unlocked workstations, and connecting to the network itself. Organizations are much more likely to have external IDS/IPS sensors installed than internal sensors, not have strong internal system controls like their external systems and not have subjected their internal systems to the same hardening process as their external systems. This allows an attacker to have free reign with a greatly reduced chance of being detected and a greater chance of system compromise.

Impact of SANS Training on the Situation

The greatest benefit of the SANS training is the broad coverage of security topics covering the 10 domains of security as outlined in the CISSP Common Body of Knowledge (CBK). This allows a student to understand how a weak control in one area, such as physical security in this case study, can lead to a greater risk in security for another area, such as the internal network. An attacker typically looks for the easiest and shortest path to their target. It also illustrates how important it is to practice security in all areas – even your 'trusted' internal network. Accepting the idea that security may fail in one area means you need it in all areas. This leads to the practice of defense-in-depth.

During

Casing the Premises

After checking into our hotel Sunday night, we proceeded to drive around the sides of the bank in order to identify all egress and ingress points as well as possible weaknesses in those points. The front door to the bank faced the main street which is well-lit and subject to foot and car traffic – including local law enforcement patrols. The back of the bank was accessible from an alley off a side street and had a smoking area that we identified as a possible point of a piggy-back attack. One side of the bank had no access points since it shared a brick wall with another business. The other side, located on a side street, has an employee entrance that is much less trafficked. The glass door used a pushbutton combination lock[6] that requires pushing a special sequence to open. All first story windows were noted to be checked as well as climbable means to access any 2nd story windows that are more likely to be unlocked.

We decided that the employee door would be the easiest point of entry. If we could ascertain the combination, it would be unlikely that someone would question our entry. Early Monday morning, we parked a SUV with tinted windows at an angle across from the employee entrance and setup a home mini-DV camcorder on a tripod so we could videotape an employee entering the combination. Within 15 minutes, we had successfully captured the sequence and validated it through playback. The code was only three digits long and was based on a easily guessed pattern. We further determined that there was a a glass door with a key lock secured by a proximity card reader at the same level as the employee entrance with stairs just inside the door that let to the 2nd story of the bank and to the basement.

Building Diagram

In order to help visualize the building layout, the progression of events, and key points, the legend below and the following diagram have been provided.

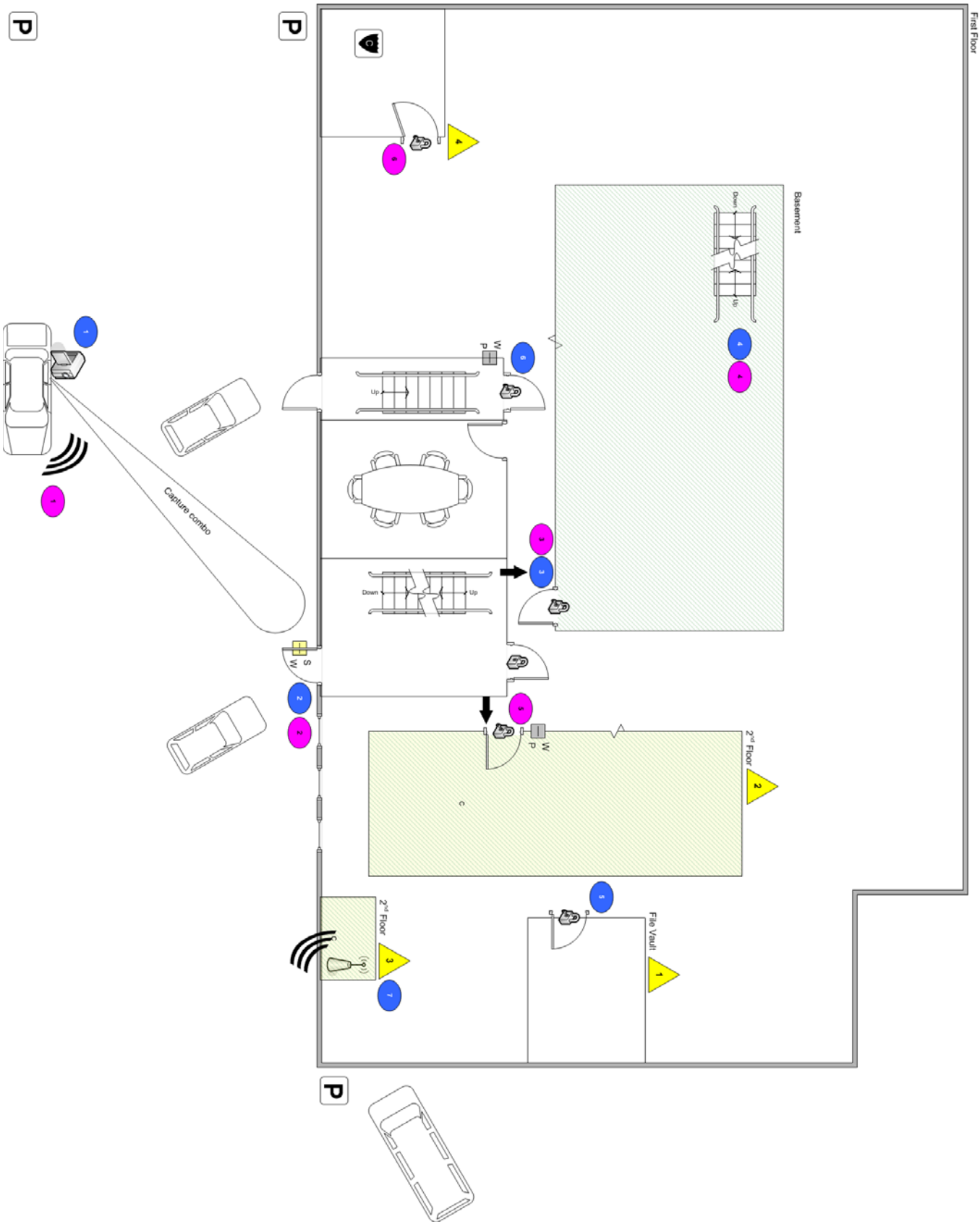
Diagram Legend

First Day Activities	**Second Day Activities**
Points of Interest	**Wireless Access Point**
Lock that was Picked	**Lock that was NOT Picked**

Points of Interest
Mortgage Room
Wireless Device
Key Stroke Logger
Chief Security Office

NOTE: See following page for diagram.

Figure 1 - Building Diagram



The First Try

In order to limit our contact with personnel, we waited and returned to the bank around 9:00 PM. While one team member monitored the employee entrance, two team members entered through the employee entrance dressed in suits in order to appear as professionals. From a social engineering perspective, their modus operandi, in case they were approached, was to impersonate auditors which would have authority to be at the bank during off-hours but may not know all the personnel or the premises. The stairs to the 2nd floor led to another glass door with a key lock secured by a proximity badge reader and well-lit. The stairs to the basement led to a wooden door with key lock, no badge reader, and poor lighting.

The basement door was picked as the next point of attack. Since it was a less used entrance and poorly lit, it would be easier to work on the lock and not be seen doing so. Additionally, since the door was old and was not upgraded to the proximity system, the lock had been used more. This results in the cylinder locking mechanism being more 'broken in' (no pun intended) and typically not as complex, hence easier to pick. As a result, the lock was picked in under 5 minutes and access was gained to the basement.

Once inside, the team found another set of stairs leading to the first floor of the bank. Also, the cleaning crew was still present. While hiding in the basement, the team had a close encounter with the cleaning crew that accessed the basement to dispose of trash. After the crew left, the team gathered customer documents from bins with materials staged for shredding. The decision was made to leave the bank until the cleaning crew had left to prevent any possible contact. Later discussions with the bank indicated the cleaning crew was a third party company and would have likely been easily bypassed through social engineering. The team returned around 11PM and gained access to the bank again.

Sweeping the Building

Some team members proceeded to assess the desk areas for all personnel. About a half-dozen proximity badges were found throughout the first floor, though none of them could open the doors since they lacked the privilege to do so at that time of the day. At the same time, any keys found were noted and some were tried, resulting in access to other areas such as the mortgage storage room. And finally, we searched for any possible usernames and passwords that might be written down. Once again, we had multiple findings in desk drawers and under desktop mats.

While this sweep was being performed, other members continued to map out the facility and attempt to pick locked doors to gain entry to new areas. One door

picked included the previously mentioned mortgage room. One of the second floor doors that was secured by a proximity badge could also be picked and allowed access to the second floor, which contained most of the banks computer operations and C-level offices. Two data centers were found, both with doors that were secured with a combination biometric/proximity badge system. Our team was unable to pick these locks and gain physical entry to the data centers.

Throughout the sweep, the team also tried to identify any unlocked terminals that might allow access to the network. We were unable to locate any unlocked systems. After the covert portion of the engagement was concluded, we learned that this was surprisingly a manual process and not automatically enforced by system policy. Apparently, any employee who leaves their desktop unlocked may be susceptible to an email being sent to an executive notifying them of the incident. We did, however, notice that the username of the last login was still displayed which could significantly reduce any login attacks since only the password is needed at that point.

Proof of Concept

During the first night's intrusion, we set out to accomplish our primary goal of showing some of the methods an attacker might use to gain IT access through bypassing physical controls.

Our first step was to install a WAP. We used a $10 5-port switch, a $10 power strip, and a $65 WAP. The strip was necessary due to a lack of available outlets. The switch was necessary to tap an existing computer's network access port. We chose a WAP with 802.11a/b/g capabilities and WPA encryption. The 802.11g protocol would allow the greatest speed at 54Mbps if the signal strength was good. The 802.11b protocol would allow the greatest range since we had an 802.11b PCMCIA card with 12db gain bi-directional antenna. The WPA encryption ensured that our activities could not be intercepted by anyone else. Other settings on the WAP included disabling the broadcast SSID so only we could see it, using DHCP on the network-facing Ethernet port, and setting up all wireless connections to NAT through that port.

In order to achieve the best signal strength, we looked for an office that was located against the wall that faced the aforementioned side street. As it happened, there were three offices on that wall with desks that had enough room behind them for the WAP and would not allow the WAP to be easily seen. One of these offices was the Director of IT, who was involved in the engagement. So, of course, we chose the office right next to his as part joke but also to prove the point.

The second step was the install a keystroke logging device since no software could easily be installed with the terminals locked. We used a 512K in-line

PS/2- based KeyLogger Standard from KeyGhost[7]. This device is accessible through a menu only after you have successfully entered in the password while using any text editor. Once entered, a menu is displayed that allows you to dump the memory, change the password, etc.

Throughout the facility, we found most of the systems could have the keystroke logger installed. Some of the issues included laptops, USB-based keyboards, or too much exposure of the device to public viewing. Eventually, we chose a desktop that belonged to a bank VP without any of the restrictions.

We left the facility at roughly 2AM with our first night activities and goals completed and our devices successfully installed.

Wireless Access

We returned the following morning about 8AM and parked on the side street next to the bank. We had a DC-to-AC converter that plugged into the vehicle's cigarette lighter and provider ample power for our laptops. For the next 4 hours, we were able to access the WAP without any wireless interference and no interruptions from any pedestrians or police. The goal was do some basic network discovery to show what might be done via the WAP access.

The exception was a visit from one of the bank employees that was aware of the covert activities and was looking for us. This employee later confirmed that he found the WAP through tracking its IP address and MAC address on their switches at roughly 4PM, well after we were done. However, he admitted he would not have typically noticed the device.

While we were connected to the network, we were able to enumerate a great deal of information about the internal network. As commonly found on internal networks, NetBIOS was not locked down on the Windows servers, which allowed us to determine all the administrator accounts, all the user accounts, and all the accounts without passwords. This was accomplished through a mix of tools including the DOS command 'net'[8], Windows 2000 Resource Kit[9] and DumpSec[10].

The biggest finding and concern was a server found with a null Administrator password. This server also allowed anonymous FTP access. Later, during the overt network auditing activities, we learned that this server was maintained by a third-party vendor and not the bank. It served as a reporting tool for all the banks accounts. We were able to ascertain usernames/password to access the accounts database as well all the bank customer account numbers and their current balance.

The Second Night

We returned the following evening about 11PM. We wanted to verify that we could repeat our success in bypassing the physical controls, collect the WAP and keystroke logger. We were able to get back into the bank through the same process as the previous night and get the WAP.

The keystroke logger went undiscovered and was successfully retrieved. We access the logs and were able to get the VP's username and password to the network. We used this to log on to her workstation and, upon noticing the VNC application, gather her password hash from the system registry. This was inputted to Cain v2.5[11], a password cracking utility, and broken. As luck would happen, we later found out that we had chosen the VP who happens to be the administrator of the bank's central accounting application.

For the second night in a row, we noticed that the Director of HR had left her laptop unsecured in her office with the door unlocked. Typically, the head of HR has very sensitive information including employee confidential information and payroll information. We removed the laptop and placed it in the office of one of our banks contacts with a note and a voicemail indicating our removal. The next morning, this removal had the intended effect of panic and the point was well made. The laptop hard drive lacked any encryption controls and could have easily been accessed by placing the hard drive in an external USB enclosure.

To help understand the impact of having additional insider information from a disgruntled employee, we invited a member of the bank's audit department to join our team this night. This auditor was able to immediately point out filing cabinets with important documents including customer signature cards and certificates of deposit – all of which were unlocked and unsecured.

Once again, we left the bank about 2PM.

After

The Next Morning

The following morning, we went back to the bank to meeting with our bank contacts and present our initial covert findings and plan out our overt activities for the next two days. We proceeded to enter the bank through employee entrance with the code we had obtained. We noticed that the first floor door, secured by proximity badges, was wedged open during the day. This explains why many first floor employees left their badges in their desks – they only needed the push-button code or use the customer entrance to get in and out of the building during the day.

We proceeded to go up to the second floor of the bank, where our contacts were located. We were able to gain access to this floor thanks to a very nice bank employee who held the door open for us, hence bypassing the proximity badge reader. After somewhat surprising our contacts, we sat down and present out findings to them and the bank president.

Physical Recommendations

We started with the pushbutton lock on the employee entrance. We later found out that the code had not been changed in over year. We recommended that it be changed on a regular basis and on key events such as the dismissal of an employee. Additionally, the pad should include some concealment to deter from public viewing. The entrance was not subject to video surveillance and was recommended to be included.

To further secure the area immediately inside the employee entrance, we recommended placing a proximity reader, new lock, and lighting on the basement entrance. Additionally, we discouraged the practice of wedging the first floor door open and encouraged proper use of the proximity badge readers. And finally, we recommended increased user awareness training about letting unknown people through doors to help prevent piggy-back or tailgating access[12].

Within the bank, we recommended they implement a data classification system and procedures to ensure that sensitive documents are secured during business hours and especially after hours. This was to address the unlocked filing cabinets containing items such as the customer signature cards. As part of this philosophy, we suggested the use of locks on the offices of key personnel such as HR as well as procedures to enforce the locking of these areas.

Though the need to test the cleaning crew used by the bank was not present, we were told that these services were performed by a third-party company. Given the lack of control over the individual employees, combined with areas that the crew may access, we recommended a clean desktop policy as well. Or as stated by a bankersonline.com article, “Don't assume your cleaning people can't read - or use your copier. Clear off your desks when you leave.“[13]

And finally, we once again recommended more user aware training in other areas. One area was the identification and notification of suspicious devices to help prevent keystroke loggers and rogue access points. Another area was the placing of usernames and passwords in unsecured areas.

Technical Recommendations

Since the first part of our engagement, and the focus of this case study, is focused on physical security, we limited our recommendations on the technical

recommendation to those of the servers discovered during the wireless vulnerability assessment.

Regarding the network servers, we recommended they develop a minimum security baseline (MSB) which includes hardening of these systems. As part of their corporate security policy, we recommend that they make sure all third-party servers meet the same MSB. Through their servers, they can also use an automated method of locking workstations, such as through Windows Group Policy Objects (GPO)[14].

Solution Impact

In accordance with the bank's corporate security policy and multiple compliance standards, they require a "Segregation of Duties"[15] in their audit controls separating their assessment work from their implementation work. This prevents any one entity from handling all aspects of the controls and any possible inappropriateness that may occur from such a situation as well as increased error detection. Therefore, my company was not a party to or made privy to the final solution and its impact.

However, our initial feedback from the customer was very positive in many ways. When the findings of the covert activities were made, they had an immediate impact on the organization just in user awareness. Ultimately, the bank was going to use these findings to help justify and drive additional resources to mitigate many of the risks we identified.

To date, the bank is an ongoing reference for our company and has stated their intention to approach us in the future for additional security assessments.

Conclusion

What occurred at this Midwest bank is not a unique situation and could occur at any other organization. In fact, a very similar event, including the installation of a WAP, occurred at a major Israeli bank that resulted in a loss of approximately $13,000[16]. It was only the detection of fraud that led to the discovery of the WAP – well after the damage had already occurred. Given the anonymity the WAP provided, the perpetrator was not caught.

Like many other things in the world, security can also be subject to trends and patterns. Prior to computer networking, the focus of an organization's security was physical controls. Especially with the development of the Internet, security saw a major growth in technical controls with the focus at the network's perimeter. Today, technical security has matured to a point where firewalls are as common as routers and the current focus is on multi-layered or 'defense in

depth' moving towards intrusion detection/prevention at both the network and host level.

These controls are usually developed and implemented as a response to the current methods and approaches of the attacker. With the perimeter technical controls becoming increasingly difficult to bypass, the attacker is likely to find the easiest and simplest method to circumvent the perimeter. This trend points to a need for organizations to go back and review their physical controls, which may have taken a backseat to the focus on technical controls. When an intruder has physical access to your organization and its assets, very few technical controls can stop them. As restated in a bankersonline.com article, "By securing your facilities appropriately -- those buildings that provide a safe haven for employees and customers, and those that contain your critical assets and records -- you deny the thug the only thing that he/she really needs to hurt you: ACCESS."[17]

And despite all the physical controls that the Trojans had in place, even they were circumvented through some good, old-fashioned social engineering. The inherit human nature to trust others and to not confront others can have a huge impact on an organization.

A final warning can be found in my favorite part of Virgil's *Aeneid*, "luna premit suadentque cadentia sidera somnos." [18], is a line describing the city the moment before the Greek attack as the citizens are passing out from their party. It can be translated as "… and moon closely followed the falling stars persuaded sleep."[19] All too often, an organization become too complacent with security and awareness can dwindle. That is the likely point when they can get lulled into a false sense of security and get caught sleeping.

References

[1] whatis.com http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html

[2] classics.mit.edu http://classics.mit.edu/Homer/iliad.html

[3] classics.mit.edu http://classics.mit.edu/Virgil/aeneid.html

[4] Global Information Security Survey 2004 Ernst & Young, Page 2 http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf

[5] Global Information Security Survey 2004 Ernst & Young, Page 5 http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf

[6] Kaba, LTD. http://www.kaba.co.uk/pushbutton/whatis.htm

[7] KeyGhost http://www.keyghost.com/kgstd.htm

[8] computerhope.com http://www.computerhope.com/nethlp.htm

[9] Microsoft.com http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp

[10] systemtools.com http://www.systemtools.com/somarsoft/

[11] oxid.it http://www.oxid.it/cain.html

[12] Newton Security, Inc. http://www.newtonsecurityinc.com/piggyback.htm

[13] Pretend You're a Crook, Barbara Hurst, http://www.bankersonline.com/security/bi_sec0430a.html

[14] Microsoft.com http://support.microsoft.com/default.aspx?scid=kb;en-us;195655

[15] University of Utah, Internal Audit http://www.utah.edu/Internal_Audit/segregation_of_duties.htm

[16] Social Engineering and Physical Security Concerns in Financial Institutions Following the Israeli Bank Hack, Gadi Evron, http://www.bankinfosecurity.com/?q=node/view/712

[17] Are You Running With Scissors? Physical Security: What You Should Be Doing Now! , Dana Turner, http://www.bankersonline.com/security/runningscissors.html

[18] Aeneid, Virgil, Book IV, Line 82 http://www.geocities.com/alspoli/classicos/eneidaiv.html

[19] Translation from Latin by Matthew T. Davis. Special thanks for William Preuter, my high school Latin teacher who assigned Book IV of the Aeneid my senior year.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event