The DEF CON 22 Social-Engineer Capture The Flag Report

www.social-engineer.org

sectf@social-engineer.org

Written by: Michele Fincher & Chris Hadnagy

Table of Contents

Table of Contents 2
Executive Summary 3
Overview of the SECTF 4
Background and Description 4
Description of the 2014 Parameters 6
Target Companies 6
Competitors 7
Flags 8
Scoring 9
Rules of Engagement (R.O.E) 10
Results and Analysis 10
Open Source Intelligence Gathering 11
Pretexting 16
Live Call Performance 17
Final Contest Results 20
Discussion 24
Mitigation 25
A Note About The Social-Engineer Village 27
Conclusion 27
About Social-Engineer, Inc 28
Sponsors 29

Executive Summary

Social-Engineer.org hosted the Social Engineer Capture the Flag (SECTF) contest at DEF CON 22 in Las Vegas, Nevada for the fifth year in a row in August of 2014. This year's competition had the added complexity of requiring contestants to work in teams of 2, necessitating pretexts that allowed for the caller to be handed off without raising suspicion.

From an original 70 entries, we selected 9 teams of 2 from diverse backgrounds and experience levels to test their social engineering abilities against specific Fortune 500 or larger companies. Below is a table highlighting some basic statistics from this year's competition:

Target Companies	9
Contestants	18
Completed Calls	121
Total Points Scored on Reports	1407
Total Points Scored on Calls	5306

Table 1: Overview of the CTF

As in years past, the overall goals of this contest were to raise awareness of the ongoing threat posed by social engineering and to provide a live demonstration of the techniques and tactics used by the potential malicious attacker. There were very strict rules of engagement in place to ensure no sensitive information on companies or individuals was disclosed. To further protect employees of target companies from potential negative repercussions, identities of those contacted is not retained.

It is important to note that the reporting of a company's overall performance is a combination of points scored by their assigned teams in both Open Source Intelligence (OSINT) gathering and live call phases of the contest. The scoring alone contained within this report does not necessarily indicate that one company is less secure than another company. However, it is an indicator of the potential vulnerabilities that exist and demonstrates that despite training, warnings and education, social engineering is still a very serious and viable threat to corporations.

Overview of the SECTF

The Social Engineer Capture the Flag (SECTF) is an annual event held at the DEF CON Hacking Convention in Las Vegas, NV. The SECTF is organized and hosted by Social-Engineer.Org, the noncommercial, educational portion of Social-Engineer, Inc.

The competition was formed to demonstrate how serious social engineering threats are to companies and how even novice individuals could use these skills to obtain damaging information. The contest is split into two iterations, the information-gathering phase that takes place prior to DEF CON, followed up by the live call phase that occurs at the DEF CON conference.

Background and Description

The SECTF is a contest in which participants attempt to obtain specific pieces of information, called flags, from select private-sector companies. The purpose of the contest is to demonstrate how much potentially damaging information can be freely obtained either through online sources or via telephone elicitation.

Months prior to the DEF CON event, we solicited for individuals who wished to compete via our social media outlets and www.social-engineer.org website. This year we required participants submit a 90-second video outlining their goals for the contest. Our panel made selections based on a number of factors to include desire to learn as well as our perception of the contestant's intent. As this is an educational event, we wish our participants to have a very strong emphasis on ultimately helping the status of corporate security as opposed to the singular goal of "winning" an engagement. This year we also added complexity to the competition by requiring that contestants work in teams of 2 and "tag out", or pass the call off to their teammate at least once during each call. We anticipated that this would necessitate the development of creative pretexts that allowed team members to tag out without raising the suspicion of the target. From 70 applicants, we selected 18 contestants divided into 9 teams of 2, and randomly assigned them to a company.

Based on major trends and breaches during the year, we selected all retail organizations as target companies this year. These are brands that US customers rely on regularly that have access to both personal and financial information of the average consumer.

Contestants were not made aware of any other competitors outside of their teammate prior to their show time at the event.

In addition, we again sent all flags, rules, targets and other pertinent information to our contacts at the Electronic Frontier Foundation (EFF), https://www.eff.org. The EFF has assisted us from the first year and every continuing year to ensure we are staying within the legal boundaries we have set for ourselves when we started this competition.

Teams were given three weeks to gather as much information about their target company as possible and generate a report. They were allowed to use only Open Source Intelligence (OSINT) that could be obtained through Google, LinkedIn, Flickr, Facebook, Twitter, WhoIs, etc. During this information-gathering phase, teams could attempt to capture as many of the pre-defined flags as possible. The information gathered was to be assembled into a professional social engineering report. Teams were provided with a sample report to assist them, but were not required to use this template. In addition to the flags, points were also awarded based on the professionalism and quality of the report submitted.

Teams were then assigned a time slot to perform their live calls on either Friday or Saturday during DEF CON 22 in Las Vegas, NV.

Great care was taken in the development of the contest to ensure maximum success for the contestants. Since the contest was held on the West Coast, companies whose headquarters were located on the East Coast were assigned earlier time slots. Furthermore, companies who were easily accessible during non-standard business hours, such as retail, were assigned Saturday time slots.

Team members were placed together in a soundproof booth and required to provide a list of phone numbers (obtained during the information-gathering stage) at the target company. This year we did not allow caller ID spoofing.

The team was free to use their entire allotted thirty-minute time slot to perform as many or as few calls as they wished. Although United States federal law only requires one party to be notified in the event of recording a telephone call, many states (Nevada included) have created additional laws requiring both parties to consent. Since we could not obtain the consent of target companies without jeopardizing the integrity of the contest, no recording of any type was permitted (including that by the audience).

Scoring was accomplished during each call by two judges. This year we also took time after each team to analyze the calls with the audience. During that time, we discussed the success of the calls, techniques used, and answered as many questions from the audience as time allowed. Subsequent to the contest, scoring and comments were reviewed along with the reports submitted prior to DEF CON to determine the winners.

It should be noted that all contestants were required to place a $20 *fully refundable* deposit to reserve their spot at the contest. All contestants were refunded this deposit immediately after completing their call at the DEF CON portion of the contest.

Description of the 2014 Parameters

Overall, we attempt to keep the *major* parameters of the competition as consistent as possible from year to year. However, we do make changes to ensure that the contest continues to be challenging and educational for both contestants and audience. This year, the major change to the format of the competition was the requirement to work in teams.

Primary changes:

- Contestants were required to work in teams of 2 and to "tag out" at least once during each call
- The contestants were allowed 30 minutes to perform their calls
- No spoofing was allowed
- Teams were given three weeks for OSINT collection and reporting (over previous years' 2 weeks)
- The target companies were all retail organizations
- Post-call analysis was provided to the audience as time allowed

Target Companies

The Social-Engineer staff, through an open nomination and voting process accomplished target selection. We made every attempt to ensure that no bias was introduced through attitudes or preconceived notions regarding any particular company. In general, we attempted to select Fortune 500 or larger companies from retail brands that are used by most average US consumers throughout the year. Although the overall security of all companies is important,

we felt an emphasis on retail (and even more specifically companies who deal directly with point-of-sale) was especially crucial since we as customers provide them access to personal information such as birth dates and credit card information. As in previous years, we made the call for companies to be willing participants in the SECTF. No companies volunteered; therefore none of the companies chosen were aware of their selection prior to the DEF CON conference.

The target list (in alphabetical order):

1. Costco
2. CVS
3. Home Depot
4. Lowe's
5. Macy's
6. Rite Aid
7. Staples
8. Walgreens
9. Wal-Mart

Competitors

As in all previous years, one of our core rules is that ***no one*** is victimized. This includes those who choose to participate, those who are called, and the companies they work for. Our contestant's personal information is never revealed and they are only photographed if they provide explicit verbal permission prior to their live call segment at DEF CON. No video recording of contestants is ever permitted.

There were 18 contestants selected from an original pool of 70 applicants. Not all were skilled callers or experienced social engineers. For many, this was their first attempt at ever placing a deliberate social engineering-based call. Some of the contestants were red team or security specialists, but many more were from other fields not related to social engineering or information security.

Another interesting fact is that not all applicants were from the U.S. This year we selected 4 contestants from outside the US to compete.

Finally, the tag-team requirement encouraged unique dedication and cooperation between team members this year. One contestant actually flew across the country to work with her teammate prior to the competition.

Flags

A "flag" is a specific piece of information that the contestants attempted to obtain in both the OSI and live call portions of this competition.

The following table outlines the list of specific flags, their categories, and point values for 2014:

DEFCON 22 SECTF Flag List		
Logistics	**OSINT**	**CALLS**
Is IT Support handled in house or outsourced?	3	6
Who do they use for delivering packages?	3	6
Do you have a cafeteria?	4	8
Who does the food service?	4	8
Other Tech		
Is there a company VPN?	4	8
Do you block websites?	2	4
If website block = yes, which ones? (Facebook, Ebay, etc)	3	6
Is wireless in use on site? (yes/no)	2	4
If yes, ESSID Name?	4	8
What make and model of computer do they use?	3	6
What anti-virus system is used?	5	10
Can Be Used for Onsite Pretext		
What is the name of the cleaning/janitorial service?	4	8
Who does your bug/pest extermination?	4	8
What is the name of the company responsible for the vending machines onsite?	4	8
Who handles their trash/dumpster disposal?	4	8
Name of their 3rd party or in house security guard company?	5	10
What types of badges do you use for company access? (RFID, HID, None)	8	16
Company Wide Tech		
What operating system is in use?	5	10
What service pack/Version?	8	16
What program do they use to open PDF documents and what version?	5	10
What browser do they use?	5	10

What version of that browser?	8	16
What mail client is used?	5	10
Do you use disk encryption, if so what type?	5	10
Fake URL(getting the target to go to a URL) www.seorg.org	13	26
Employee Specific Info		
How long have they worked for the company?	3	6
What days of the month do they get paid?	3	6
Employees schedule information (start/end times, breaks, lunches)	3	6
What is the name of the phone/PBX system?	4	8
When was the last time they had awareness training?	5	10
Report Scoring		
Half points for any flag found from information gathering	**	**
10 points each for each realistic attack vector detailed in the report to a maximum of 50 points. Supporting evidence must be provided for each attack vector as to why it is realistic.	10-50	
Format, structure, grammar, layout, general quality of the report a maximum of 50 points.	0-50	
Call Scoring		
For every successful TAG OUT to your partner		10

Table 2: Flag List for 2014

Scoring

Contestant report scoring for the OSINT phase was accomplished manually using the guidelines from Table 2. Flags obtained during this phase of the contest were worth **half-points.**

Scoring during the live telephone calls was accomplished using a proprietary application specifically designed for Social-Engineer. Flags captured during this portion of the event were awarded full points (please see Table 2). The same flag could be captured multiple times by the same team by contacting different targets within the allotted thirty minutes. For example, if the team reached three different people and convinced all three to navigate to the website of the contestant's choosing (a flag worth twenty-six points), they would have received seventy-eight points. Every attempt was made to ensure consistency in scoring for all teams, regardless of the judge, although our scoring process does provide some subjectivity through the ability to include notes and comments for each contestant.

This year required our contestants to work in teams and "tag out" during their calls. This means that each team was required to pass the target off to their partner at least once during each call. Each successful tag out was awarded 10 points.

In addition to determining the SECTF winner based on points totals, we also conducted an analysis of how the target companies fared in response to a social engineering attack. It follows that the interpersonal skills and overall preparation of the contestant was highly predictive in the outcomes indicated by both scores as well as subjective assessments of performance on both sides. Unfortunately, a company cannot rely on the hope that a malicious social engineer will be inexperienced, unskilled, or unprepared upon which to base their sense of corporate security.

Rules of Engagement (R.O.E)

Contestants are held to very strict rules to ensure the protection of target companies. The core rules remained the same as in previous years. We forbid the collection of sensitive data such as credit card information, social security numbers, and passwords. Only Open Source Intelligence (OSINT) was allowed. We did not allow physical (i.e. facility) or technical (i.e. network) penetration into companies. In addition, we did not allow the contestant to visit any location of their target or interact with any person from the target before the call at DEF CON. We also specifically avoided sensitive industries such as government, education, healthcare, and finance.

The most important rule stressed to all contestants is that there was to be absolutely no victimization of any target companies. For more specific information on the ROE, please visit us here: http://www.social-engineer.org/ctf/def-con-22-sectf-registration-rules/.

Results and Analysis

This year's requirements of working in teams and "tagging out" created interesting challenges for our contestants. We anticipated that this would necessitate the formulation of unique pretexts and require close coordination between teammates. We also thought that team conditions might prove to be an advantage for the target companies during the live call phase, as people typically do not receive calls in which they are continuously passed back and forth between unknown callers.

High profile events in the last 6 months or so are illustrative of the fact that corporations, and specifically retail, continue to be extremely poor at protecting critical information. Unfortunately, this year's SECTF supported this trend as our contestants, both experienced and newcomers, dealt admirably with the team challenge. We did find some very interesting results, however, which are detailed in the sections that follow. It should be noted that any

comparisons to previous years' performance is for subjective trend analysis only. Since populations and sample sizes are not equivalent across years, statistical analysis is not appropriate and was not performed.

Open Source Intelligence Gathering

Preparation prior to any social engineering engagement is critical. It is this phase that is the most time-consuming and laborious, but can most often determine the success or failure of the engagement. The professional social engineer must be aware of all of the information-gathering tools freely available as well as the many accessible locations online that house valuable pieces of data.

The following table is a list of tools commonly used by professional social engineers as well as our contestants during the OSINT phase of the SECTF:

Google	PicasWeb	Spokeo
Maltego	WhoIs	YouTube
FriendFinder	WGet	FourSquare
Bing	Vimeo	Friendster
Twitter	Tineye	MySpace
PiPl	WaybackMachine	Google Images
Bing Images	LinkedIn	Telnet
Facebook	Monster	EchoSec
Plaxo	GlassDoor	Google Dorks
Google Maps	Yelp	BackTrack
Wordpress	Craigslist	Kali Linux
Shodan	JigSaw	

Table 3: Commonly-Used OSINT Tools

We were generally very impressed with the quality of the research, and the reporting continues to improve. One very interesting difference we found over last year, however, is that teams did not locate as much OSINT on their targets as in the past. Even accounting for differences due to team as opposed to individual scoring, points awarded in the report phase were much lower this year compared to last year's OSINT scores. In addition, there was a complete reversal from

last year in the points awarded for OSINT versus live call performance. These differences are even more astounding given the fact that overall totals between this year and last are relatively consistent, with 2013 grand total at **6,570** points and 2014 grand total at **6,713** points.

Figures 1 and 2 illustrate the complete reversal in point distribution between OSINT and live call portions between 2013 and 2014. Although our 2013 contest separated performance between men and women, one can still observe that both groups performed much higher in OSINT than live calls last year.

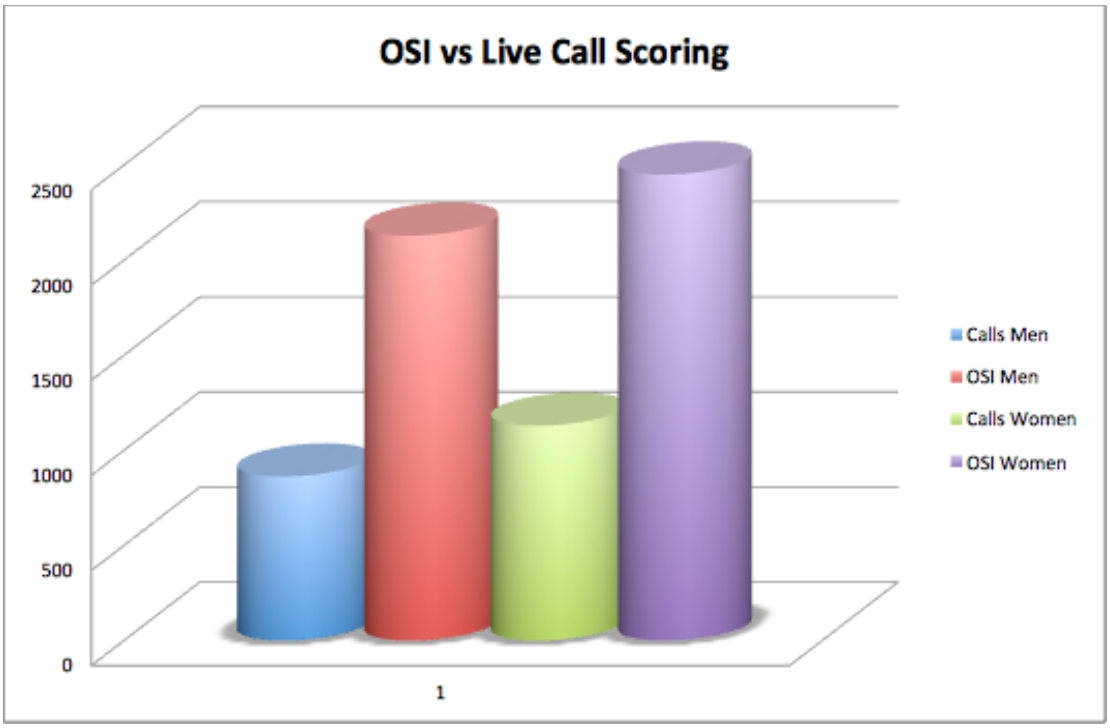

Figure 1: 2013 Total Call Points vs. OSI Points (Men vs. Women)

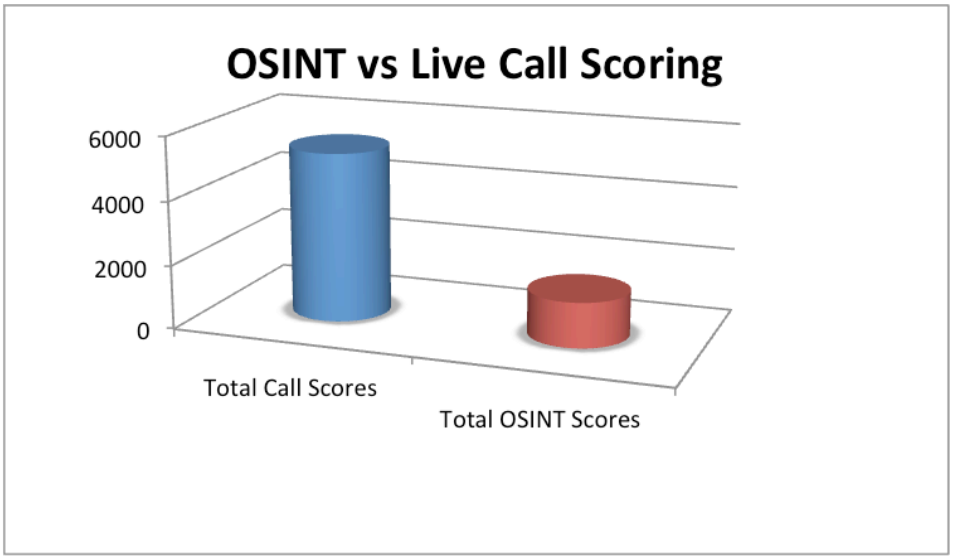

Figure 2: 2014 Total Call Points vs. OSI Points

To confirm the strength of the reversal, we examined this year's scores a bit more closely. First, we determined that the effect was still present in the absence of any extra points awarded during either phase (e.g., tag outs). Please see Table 2 for details on extra point scoring. Without any additional points, we found the difference to be even more pronounced, illustrated in Figure 3. Since there were no extra points awarded for the live call portion for the 2013 SECTF there will be no additional cross-comparison charts.

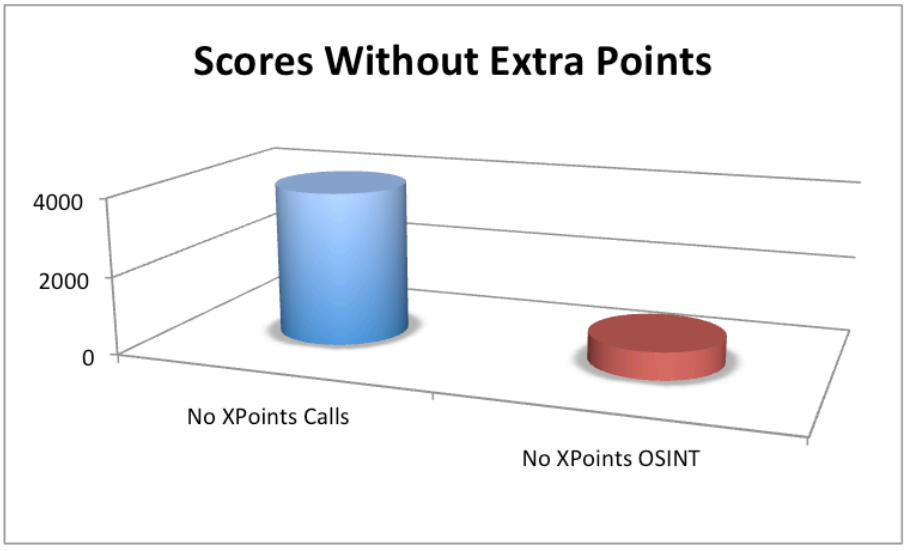

Figure 3: 2014 Scores without Extra Points

Since OSINT scores are worth half-points, we also adjusted the raw scores to ensure an equivalent comparison. Figure 4 provides a true flag to flag score comparison and confirms the strength of the effect and reversal over last year.

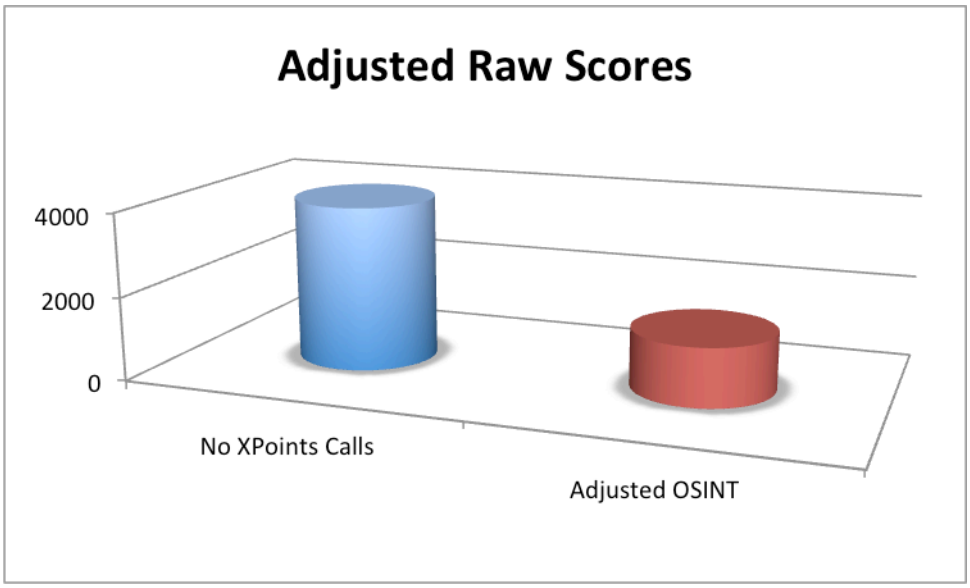

Figure 4: 2014 Adjusted OSINT Score Comparison

Looking beyond the totals, there were NO teams that scored higher on OSINT than the live call portion of the contest this year. On the surface, this may be an indicator that companies are becoming more vigilant about securing their most obvious online information. Subjectively, we do not feel that it is an indicator of the level of effort or attention to detail on the part of our contestants. Despite lower scores, the quality of information found was excellent and is still potentially very damaging to companies.

The following small list of this year's findings demonstrates that the dangers of social engineering information gathering is still prevalent:

- In one case a major retailer had a sub-Reddit set up that allowed their employees to post and discuss various topics; many included sensitive information and led to a deep understanding of the inner workings of this company.
- Another retailer had a document online that outlined the information employees would need to log into their private payment portal. This kind of list provides an attacker a clear path of information to try and obtain for an attack.

- Many companies allowed employees to post pictures of parties, badges, computer screens, break rooms and other various employee-only artifacts to popular social media sites.
- One major retailer actually listed their employee schedule on Instagram. Of course, this type of information would allow for a very personalized attack on staff.
- One contestant found a confidential document with the signature of the CEO.
- One major retailer had posted a document that openly listed their password policy as the first three letters of their company + first three letters of the employee last name and a two digit code. Of course, this means only 2 digits would need to be guessed for a compromise.
- One major finding was a publicly-available instruction manual that contained an actual working username and password for part of the corporate website.
- One contestant found numerous public postings of very disgruntled employees. This is a major threat, as enemy companies/groups would target the disgruntled to turn them.

Figure 5 provides a side-by-side comparison of points scored by teams against their assigned company during the OSINT portion of the contest. The X-axis represents the separate teams, the Y-axis the point values for flags without extra points, extra points, and totals.

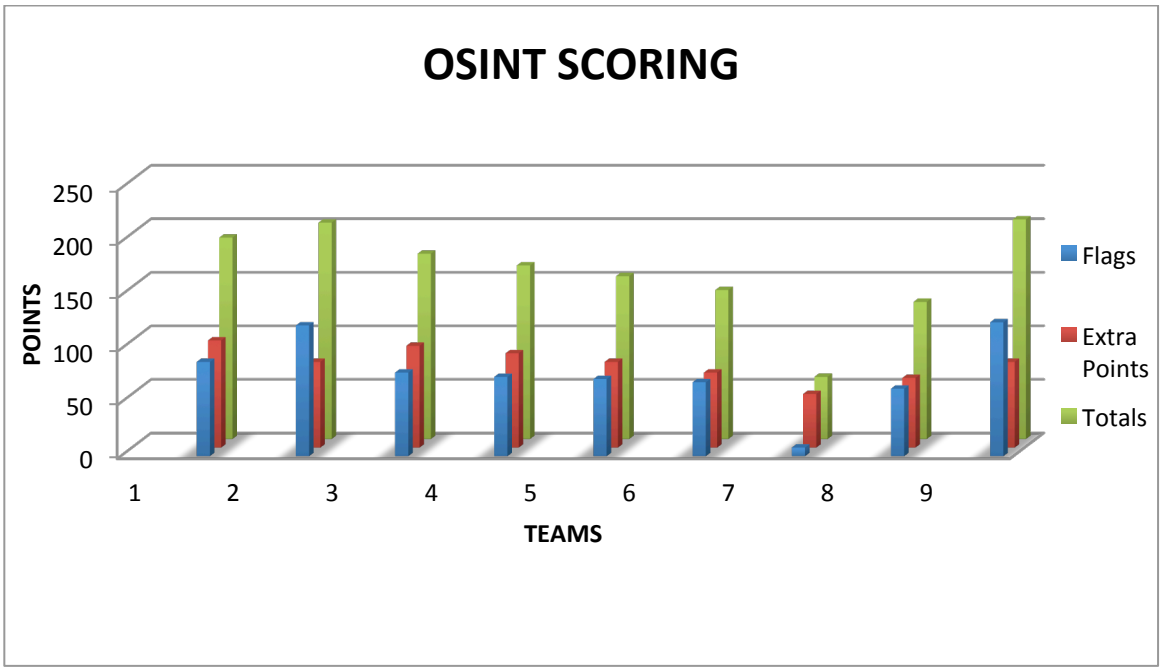

Figure 5: OSI Scores by Team

Scores notwithstanding, the OSINT portion of our competition stresses a few key points. First, this emphasizes the overall importance of the information-gathering phase of any social engineering engagement. A thorough online investigation can provide an individual with a very good understanding of when, where, and how companies conduct business as well as the online activities of their employees through vectors such as social media. Second, any images found can be extremely useful for malicious attackers attempting physical impersonation. For instance, if an attacker knows what buildings look like, the location of entrances and break areas, and perhaps even finds pictures of corporate badges, these are all potential vulnerabilities. Finally, our OSINT exercise stresses the issue of online data leakage by organizations. Network penetration was not allowed; the flags during the OSINT phase were obtained through information freely found online *without any live interaction with individuals at the target companies.*

Pretexting

The quality of pretexts used by our teams this year was excellent. All teams created believable scenarios that worked with this year's new challenges. However, we truly felt that this would ultimately give an advantage to targets based on the unlikeliness of a situation in which a person would be called and asked to give information not to just one, but two unknown callers.

We saw a continuation of last year's trend in which the vast majority of pretexts involved the impersonation of fellow corporate employees. Teams conducted an impressive amount of research to ensure any details provided were accurate and believable. There were no attempts at pretexts that have historically had poor performance such as job seekers or students asking for information.

The following figure is a more detailed breakout of the pretexts used by our contestants this year.

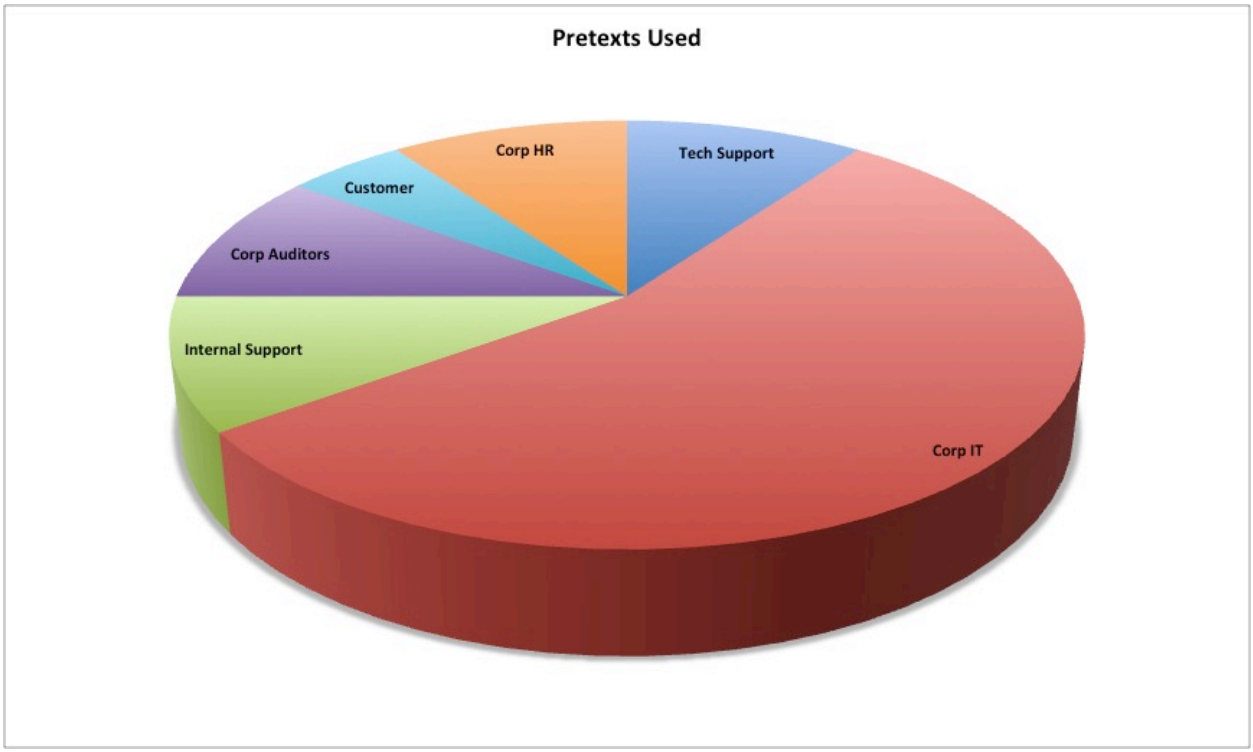

Figure 6: Pretexts Employed

It is clear that our team and tag out challenges affected the types of scenarios that could plausibly be used. The vast majority of our teams impersonated internal employees from different divisions.

Impersonating a fellow employee not only allowed teams to explain the tag out situation, but also took advantage of "tribe mentality." We inherently trust people who are part of our group or tribe. When a social engineer displays information to support that s/he is an internal employee, it is easier for the target to let their guard down and trust the person with what might normally be considered confidential information.

Live Call Performance

The live call portion of the SECTF is an interesting trial for the contestant. It is not only a test in mental agility and the ability to influence a person in real-time, but also a task that must be accomplished in front of a live audience. The luxury of time and true anonymity enjoyed in the OSINT phase are not applicable. It is for that reason we congratulate all of our contestants in completing this phase of the competition.

Figure 7 quantifies point values scored by the teams against their assigned company during the live call portion of the contest. The X-axis represents the separate teams, the Y-axis the point values for flags without extra points, extra points, and totals. The extra points awarded were based on number of successful tag outs during each call.

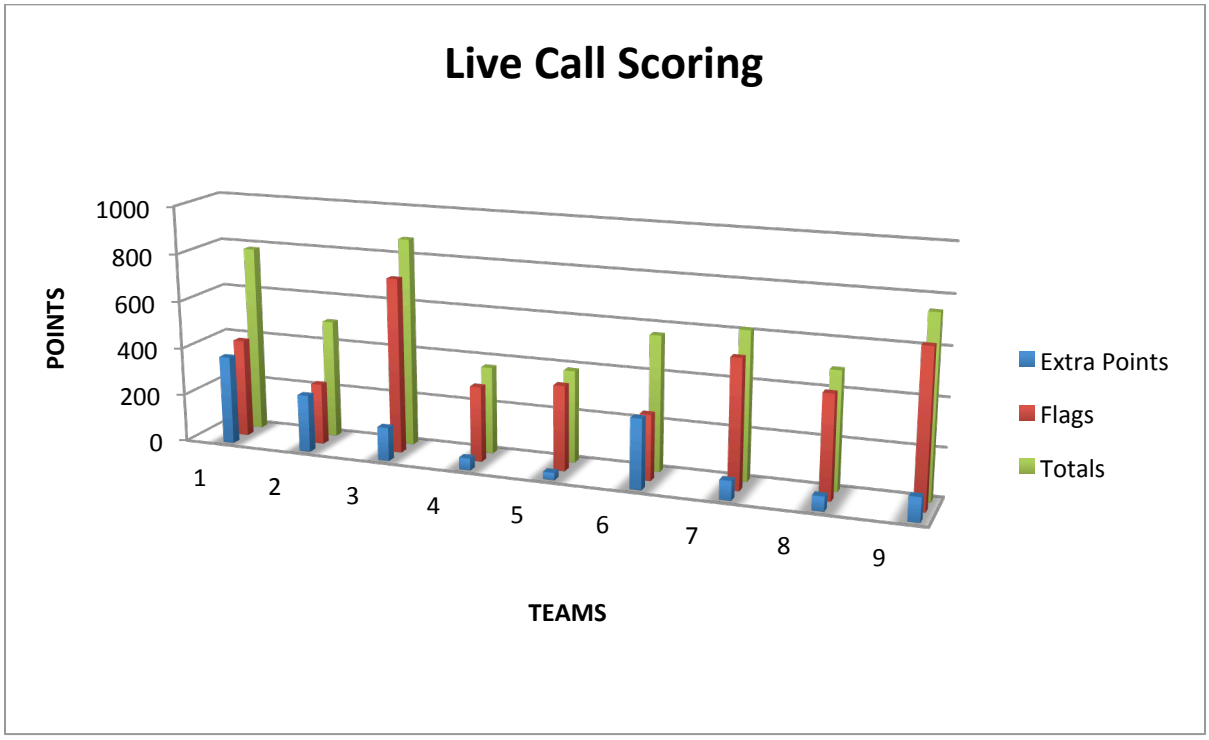

Figure 7: Live Call Scores by Team

By examining Figure 7, it is clear that most of the teams still relied heavily on obtaining points based on the flags themselves as opposed to maximizing the number of tag outs.

It is also interesting to note the vast difference amongst teams in the number of successful tag outs. The number of tag outs for each team is quantified in Figure 8.

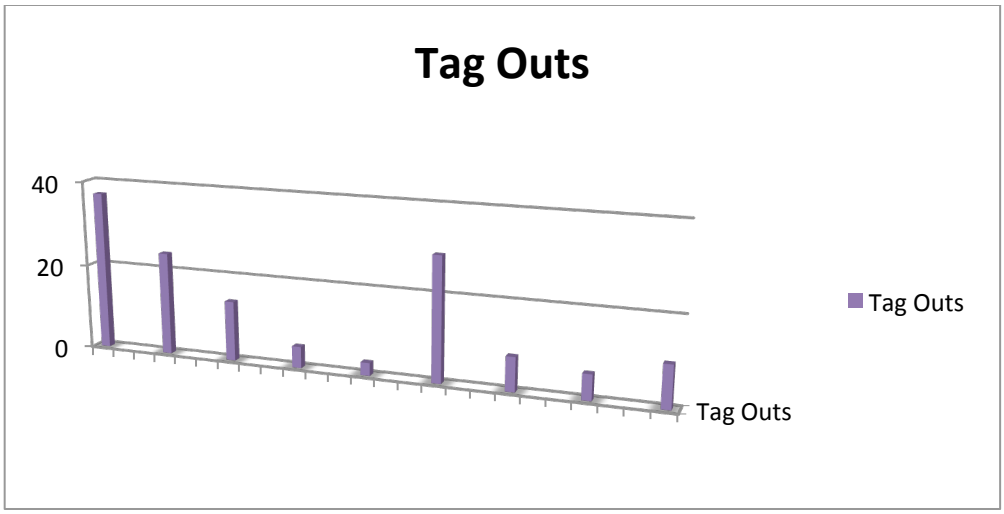

Figure 8: Tag Outs by Team

Although the range between most and least number of tag outs is very large, consider that the total time allotment for each team was 30 minutes. The mean score for this distribution is 15.11 tag outs, which averages to a call transfer every two minutes. The fact that all teams were able to successfully transfer calls and obtain flags should be noted. The implication is that even despite this unusual situation, targets still provided information to callers. In addition, most of the individuals who complied did so without asking for justification for the call transfers. Those who did still did not offer significant resistance.

The fact is that providing any justification, regardless of strength, is often enough to obtain compliance. Dr. Ellen Langer and fellow researchers found this to be true decades ago when they conducted a fascinating study in which participants attempted to cut into a line at a copy machine. They found that giving even a very weak reason ("Can I cut in line because I need to make copies?") was enough to increase compliance.

This was also supported anecdotally at the SECTF. During one of the calls, a target asked why she was on a call with two callers as well as justification for why the call was being passed back and forth. The quick-thinking contestant explained that it was for training purposes and the callers were using an Adobe Connect VoIP application. Although the target did not sound entirely convinced, she proceeded to disclose the information asked of her.

Although this answer should not have sufficed, the confidence and speed at which the answer was delivered led the target to surrender the information requested. Reviewing the live calls, we felt that the success rested with those contestants who were confident and self-assured,

knowing the information they needed quickly. The majority of the time when a lack of confidence was displayed, the target also started to lack confidence in the contestants' pretext and the call was shut down shortly after.

It is also interesting to note that our teams were successful despite not being allowed to spoof phone numbers this year.

The lesson here for security professionals and companies is the importance of teaching critical thinking skills to your organizations. Individuals need to be able to step outside of their daily workflows to analyze and ultimately make good decisions about requests that seem unusual. Many people either feel rude asking for additional explanation or readily accept whatever is offered.

Final Contest Results

At the conclusion of the live call portion of the contest, the judging panel met and reviewed all scores. The figure below is a tally of report scores, call scores, and grand total by team.

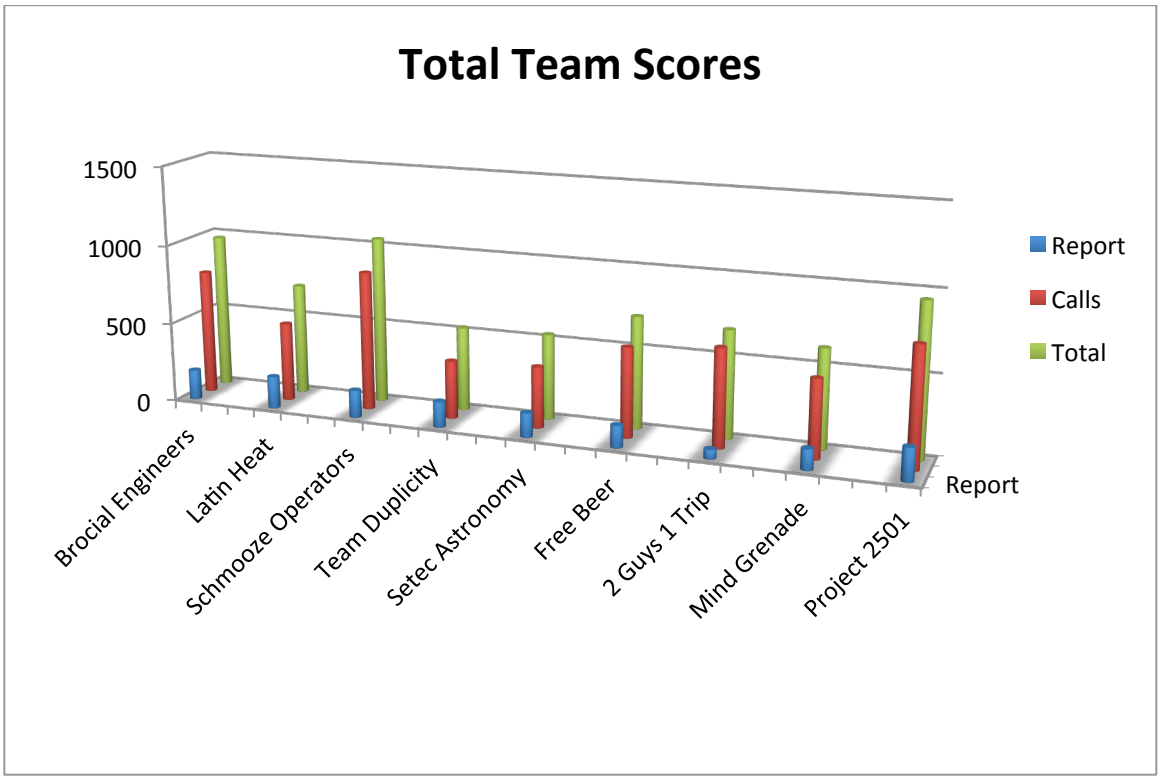

Figure 9: Total Scores by Team

Even a cursory examination of the scores confirms the heavy reliance by all teams on call scores over OSINT for scoring this year. In addition, the top three teams were very closely matched, with the difference in total scores between 1st and 3rd place only being 96 points. An interesting distinction between 1st and 2nd place teams was the use of tag outs. The Schmooze Operators relied more heavily on obtaining points directly for the flags themselves; their tag out frequency was just below the group average at 14. Team Brocial Engineers was able to dramatically increase their call score through the successful use of a staggering 37 tag outs during their 30 minute time slot.

The strategy difference between these two teams is likely due to something that tends to be a perennial issue for the SECTF, that of no-shows. We have absentee contestants every year due to a number of factors; illness, last minute nerves, etc. Since working on teams was central to this year's contest, no-shows had the potential to completely disqualify the remaining team member. The Schmooze Operators lost a team member due to illness, and the remaining contestant had a few hours to find a replacement and prepare for calls. The difference in comfort level and opportunity for prior planning may have had an impact on the total number of tag outs, but clearly the emphasis for this team was in obtaining a large number of flags.

Aside from the team rankings, the scores are directly relevant to the companies targeted in this year's competition. The figure below are the points collected by contestants in both the information-gathering and live call stages of the SECTF against their assigned companies. Please note that the higher score denotes that a higher number or value of flags were surrendered, and is indicative of poorer performance on the part of the company.

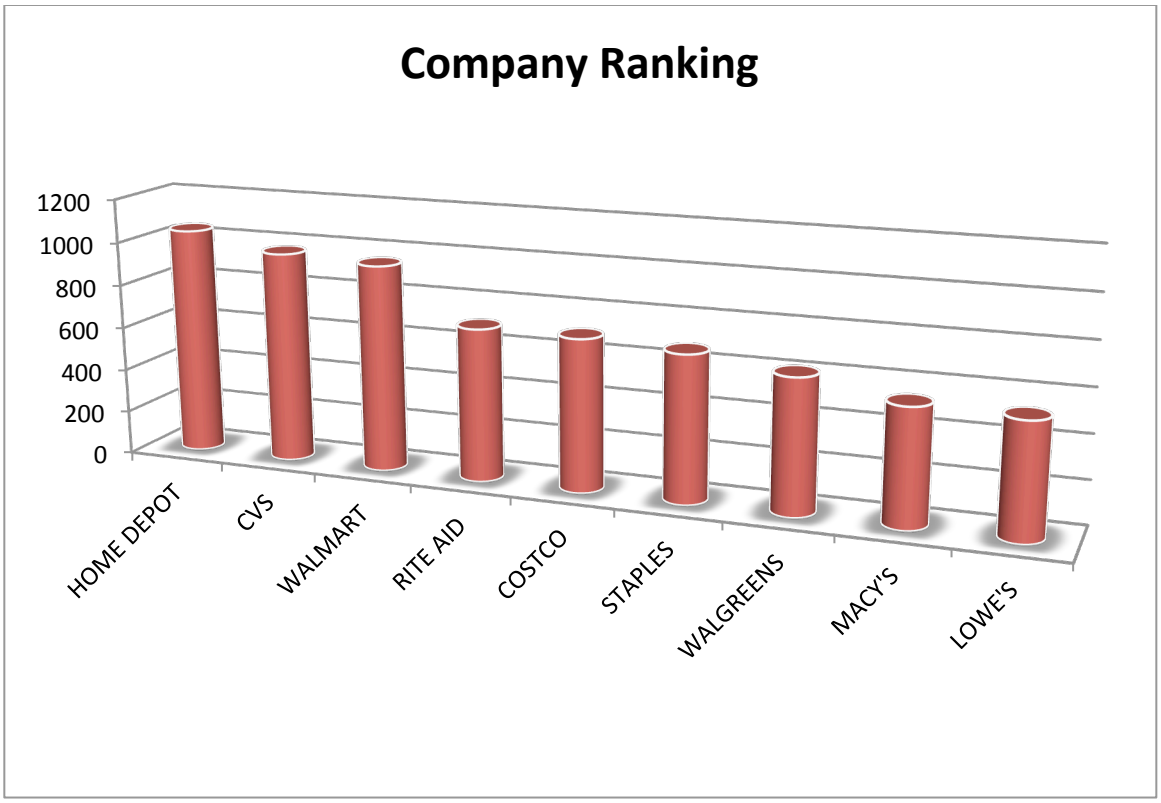

Figure 10: 2014 SECTF Target Company Performance

We do not release additional information regarding specific vulnerabilities of the companies to the general public.

NOTE - *We do provide this information directly to the involved companies upon request.*

One positive aspect of the SECTF each year is to see when a company shuts down the contestant. That is, the person from the target company follows security procedure and does not answer any questions or hangs up on the call. Each year when a person from a target company stops a contestant, the room breaks out into applause.

This year shut downs only occurred on two occasions over the entire course of the contest. Unfortunately, even after one target shut down the contestant, another call was made to the same company and another employee surrendered all the information resulting in a successful social engineering call.

Finally, Figure 11 illustrates the number of times each flag was obtained during both OSINT and live call phases. At a glance one can see that the most commonly obtained flag this year was whether there was a wireless network in place. This has obvious implications for the development of either technical intrusions and/or eavesdropping of corporate networks. With the proliferation of wireless networks, this confirms the importance that should be placed on this particular piece of technology; since out-of-the-box setup is very easy, but ensuring its security can be challenging. The take-away here is that social engineering is not always the endgame, but can be used as the entry point to perpetrate a technical attack.

It is interesting to note that EVERY flag was surrendered at least once by the target companies.

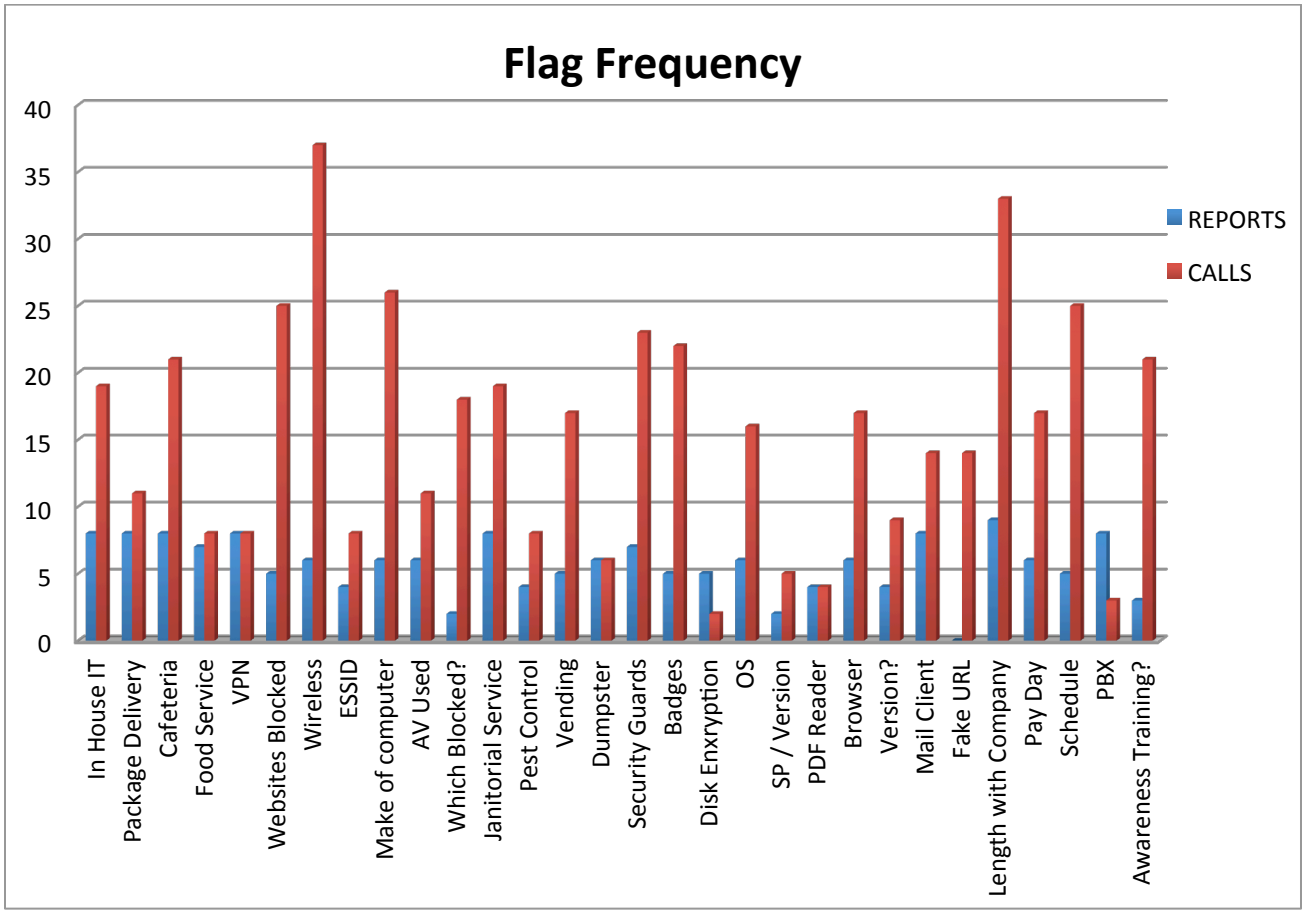

Figure 11: Frequency of Flags

Discussion

This was once again an interesting and informative year. Based on all of the data and our own observations, we can conclude a few points. First, social engineering continues to be a security risk for organizations. This is our fifth consecutive year hosting this event; in that time and despite numerous high-profile security breaches in the retail sector, we have not seen consistent improvements that directly address the human factor for organizations. The success once again of our competitors this year clearly demonstrates that potentially damaging information can still easily be obtained both online and over the phone.

Our belief that the unlikely team scenarios would provide an advantage to targets during live calls was not supported by the data. If anything, companies' performance was even worse this year, even if one compares 2014 scores without any extra points due to tag outs (Figure 3) with combined male and female 2013 scores (Figure 1). This does not bode well for the companies involved or any of us who conduct business with retail organizations.

In addition, even as companies are reportedly investing more in security awareness, we do not believe there is an appropriate emphasis on choosing awareness training that is both effective and stresses critical thinking.

Companies are still allowing sensitive data to be posted online. Individuals are still providing information to unverified callers. People are not being educated to understand the value of the information they hold or how to appropriately protect it. Rather than accept the situation at face value, employees need to be trained and encouraged to question, challenge, and make good decisions.

If that task is too difficult to overcome immediately, then at minimum, employees need to have proper protocols in place that allow them to question callers. For example, if all employees were forced to verify themselves with an employee ID or other daily code, this could greatly reduce the risk of telephone-based attacks and the need for critical thinking.

In direct opposition to security is the basic nature of conducting modern business. All companies deal with security challenges, but many of these are magnified in the retail industry. The nature of retail is such that clear communication with, and accessibility by, customers is mandatory. The typical retail customer wants the product they want, knows how they want it, and they want it immediately. This places companies in a position where they need to make their resources highly available, and perhaps vulnerable. In addition, retail employers typically deal with high turn over of employees. This provides an even greater challenge when

attempting to ensure the company is consistently trained as well as invested in corporate security.

We sincerely hope our findings are useful in making retail safer as an industry, and a secure place in which to conduct business.

Mitigation

The ongoing goal of the SECTF is to raise awareness of the threat that social engineering presents to both organizations and individuals. The crux of this report is to inform companies of the dangers associated with malicious social engineers as well as how they can mitigate and protect against these attacks.

Based on our practice and in reviewing the trends over the past several years, we would expect the use of social engineering to continue to be a significant threat to organizations. Technical controls are only part of a solution that should include ongoing education and auditing as a standard practice to defeat malicious attackers.

Below are a few suggestions for potential mitigation of this threat.

1. Defensive Actions

The open source information-gathering piece of the contest revealed how much data on a target company can be gathered through the simplest online searches. Companies must balance the business requirements of managing their brands with the risks associated with having open and approachable communications with their employees and the world. To further complicate the issue, corporate policies on information handling as well as employee social media use can often be either vague or unrealistic.

Companies need to set clear definitions of what is and is not allowed with regard to the handling and posting of information, particularly with respect to social media. Individuals will often not make the connection that personal life being discussed in an open social forum can be leveraged to breach their employers. In addition, clearly defined policies on how, where, and what kind of information can be uploaded to unsecured areas of the Internet can go a long way to safeguarding companies.

Finally, companies MUST help their employees understand what information is valuable and how to think critically about its protection. Guidelines, policies, and education can help the employees understand the risks associated with information exchange in both their personal and professional lives, creating a security-focused culture.

2. Realistic Pentesting

One of the most necessary aspects of security is the social engineering *risk assessment* and *penetration test*. When a proper risk assessment is conducted by professionals who truly understand social engineering, real-world vulnerabilities are identified. Leaked information, social media accounts, and other vulnerable aspects of the company are discovered, cataloged, and reported. Potential attack vectors are presented and mitigations are discussed.

A social engineering *penetration test* increases the intensity and scrutiny; attack vectors are not simply reported, but executed to test a company's defenses. The results are then used to develop awareness training and can truly enhance a company's ability to be prepared for these types of attacks.

We conclude that if the companies targeted in this year's competition possessed regular social engineering penetration risk assessments and testing, they might have been more aware of possible attack vectors and been able to implement education and other mitigation to avoid these potential threats.

3. Security Awareness

One of the areas that appear to be lacking across the board is quality, meaningful, security awareness education. Educating the population to meet compliance requirements is not sufficient. In our experience, there is a definite relationship between companies that provide frequent and relevant awareness training and the amount of information that company surrenders. An organization that places a priority on education and critical thinking is sure to possess a workforce that is far more prepared to deal with malicious intrusions, regardless of the attack vector.

Security awareness training needs to be practical, interactive, and applicable. It also needs to be conducted on a consistent basis. It doesn't require that a company plans large events each month, but annual or biannual security reminders should be sent out to keep the topic fresh in the employees' minds. Often, the difficulty lies in businesses making training and education a priority to the extent that appropriate resources are allocated to ensure quality and relevance. Security education really cannot be from a canned, pre-made solution. Education needs to be specific to each company and in many cases, even specific to each department within the company. Companies who truly understand the challenges and rewards associated with high quality training and education will find themselves most prepared for the inevitable.

These are just three of the many strategies that can be utilized to improve and maintain security and prepare for the attacks being launched on companies every day. Our hope is that this report helps shed light on the threats presented by social engineering and opens the eyes of corporations to how vulnerable they really are.

A Note About The Social-Engineer Village

DEF CON 22 introduced the first ever Social-Engineer Village. This year, instead of simply hosting the SECTF we created a four-day event to entertain and educate DEF CON attendees on all things social engineering. We offered a number of different contests that involved social engineering skills such as solving puzzles (critical thinking) and identifying microexpressions. We also hosted a number of presentations by well-known social engineers to provide our audience with their unique perspectives in the field, as well as our own live SEORG podcast.

Based on an overwhelmingly positive response, the Social-Engineer Village will return in 2015 and will be a major event at DEF CON 23. We will expand our contests, presentations, and plan on holding mini-seminars for those interested in learning more. We will be releasing a Call for Papers along with our call for 2015 SECTF contestants in coordination with DEF CON announcements. Please watch our website www.social-engineer.org and our social media accounts @HumanHacker @SocEngineerInc, and https://www.facebook.com/seorg.org for the most current information.

Conclusion

This was another excellent year for the SECTF. Our contestants continue to evolve and mature; time and again proving that social engineering is a skill that can be used by anyone at any level. The unfortunate finding, of course, is that based on our small sample, companies are not significantly better prepared to repel SE attacks than they were at the inception of this contest five years ago. It is our hope that this will change as we continue to expand our event and stress ongoing preparation, not just the attention garnered at DEF CON.

If you, or your organization, have any questions regarding any aspect of this report please contact us at: sectf@social-engineer.org.

About Social-Engineer, Inc

Social-Engineer, Inc. is the leading authority in the art and science of social engineering. We started as Social-Engineer.Org, an educational organization, developing the world's first social engineering framework and going on to offer the latest SE news through our blog and podcast. While maintaining this educational portion to our organization, we eventually evolved into Social-Engineer.Com, a professional training and services provider supporting customers in government and private industry.

Our goal always has been, and continues to be, "Security through Education"

Sponsors

The 2014 Social-Engineer Capture the Flag contest would not have been possible without the generous support of the following organizations:

SOCIAL-ENGINEER

www.social-engineer.com

wombat security technologies

www.wombatsecurity.com

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

www.trustedsec.com

pindrop security

www.pindropsecurity.com