Prepared by: Michele Fincher & Chris Hadnagy

The DEF CON 21 Social-Engineer Capture The Flag Report

www.social-engineer.org

Table of Contents

Executive Summary

Social-Engineer.org hosted the Social Engineer Capture the Flag (SECTF) contest at DEF CON 21 in Las Vegas, Nevada for the fifth year in a row in August of 2013. Based on continuing interest, we once again created teams of men and women to compete against one another in order to determine, among other factors, whether there was a performance difference based on gender.

From an original 198 entries, we selected 10 men and 10 women from diverse backgrounds and experience levels to test their social engineering abilities against specific Fortune 500 or larger companies. Each target company was assigned both a male and female contestant. Below is a table highlighting some basic statistics from this year's competition:

Target Companies	10
Contestants	20
Completed Calls	51
Possible Flags	37
Total Points Scored by Men	2,991
Total Points Scored by Women	3,579

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 contestant in both Open Source Information (OSI) 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.

Month's prior to the DEF CON event, we solicited for individuals who wished to participate. As a follow-up to the previous year's contest, we elected to once again pit men against women. We selected 20 contestants, 10 men and 10 women, and randomly assigned them to a company. As an organization, we attempted to select companies from a variety of industries to ensure as diverse a picture of the private sector as possible. We also placed an emphasis on brands that US customers rely on regularly since these companies would have access to both personal and financial information of the average consumer. Contestants were not made aware of any other competitors 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.

Contestants were given two weeks to gather as much intelligence about their target company as possible. They were allowed to use only Open Source Information that could be obtained

through Google, LinkedIn, Flickr, Facebook, Twitter, WhoIs, etc. During this information-gathering phase, contestants 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. Contestants 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.

Contestants were then assigned a time slot to perform their live calls on either Friday or Saturday during DEF CON 21 in Las Vegas, NV. We scheduled the time slots such that the male and female contestants were scheduled back-to-back against their specific target company and their order was decided by a coin toss for each pair.

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.

Contestants were placed in a soundproof booth and required to provide a list of phone numbers (obtained during the information-gathering stage) at the target company to call along with phone numbers they wished us to spoof. Caller ID spoofing is a method through which one's incoming phone number can be forged, or "spoofed". This is a tactic commonly used by social engineers to increase their credibility with recipients. Spoofing was not required, but was permitted.

The contestant was free to use their entire allotted twenty-five 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.

Scoring was accomplished during each call by two judges. 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 2013 Parameters

Overall, we attempt to keep the parameters of the competition as consistent as possible from year to year. This year, there were no changes to the format of the competition or how the contestants needed to prepare. We did, however, make some modifications based on past experience and feedback.

Primary changes:

- The contestants were required to provide phone numbers at the target company to call with each pretext or vector
- The contestants were allowed 25 minutes (over previous years' 20), to perform their calls
- The contestants were required to outline all OSI flags in the report to facilitate scoring
- Instead of being limited to certain industries, diverse target companies were chosen emphasizing brands that are regularly relied-upon by the consumer

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 a diversity of industries as well as 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 consumer brands was especially crucial since we as customers provide them access to sensitive 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 to be willing participants; therefore none of the companies chosen were aware of their selection prior to the DEF CON conference.

The target list (in alphabetical order):

1. Apple
2. Boeing
3. Chevron
4. Exxon
5. General Dynamics
6. General Electric
7. General Motors
8. Home Depot
9. Johnson & Johnson
10. Walt Disney

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 give permission.

There were 10 males and 10 females selected from a pool of 198 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 marketing researchers, students, house wives, sales staff and from other fields not related to social engineering or security.

Another interesting fact is that not all applicants were from the U.S. This year we selected 3 contestants from outside the US to compete.

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:

DEFCON 21 Social-Engineer.Org SECTF Flag List	
Logistics	**Points**
Is IT Support handled in house or outsourced?	5
Who do they use for delivering packages?	7
Do you have a cafeteria?	5
Who does the food service?	7
Do you use disk encryption? If so which type?	7
Other Tech	
Is there a company VPN?	7
Do you block websites? (Facebook, Ebay, etc)	3
Is wireless in use on site?	3
ESSID Name?	7
What make and model of computer do they use?	5
What anti-virus system is used?	10
Can Be Used for Onsite Pretext	
Do you have a cleaning/janitorial service?	5
What is the name of the cleaning/janitorial service?	7
Do you have an bug/pest extermination contract	5
With Whom?	7
What is the name of the company responsible for the vending machines onsite?	7
Do they have trash handling?	5
Who handles their trash/dumpster disposal?	7
Do you have a 3rd party security guard company	9
Who is it?	10
Company Wide Tech	
What operating system is in use?	10
What service pack/Version?	15
What program do they use to open PDF documents and what version?	10
What browser do they use?	10
What version of that browser?	15
What mail client is used?	10
What version of the mail client?	10
Fake URL(getting the target to go to a URL)	25
Employee Specific Info	
How long have they worked for the company?	5
What days of the month do they get paid?	5
Employee termination process?	5
New hire orientation information?	3
Employees schedule information	5
- (start/end times, breaks, lunches)	5
Do they have a PBX system?	5
What sort of phone system is used?	7
When was the last time they had awareness training?	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, grammer, layout, general quality of the report a maximum of 50 points.	0-50

Table 2: Flag List

Scoring

Contestant report scoring for the OSI phase was accomplished manually using the guidelines from Table 2. Flags obtained during this phase of the contest were worth **half-points** (please see Table 2: Flag List).

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: Flag List). The same flag could be captured multiple times by the same contestant by making multiple calls within the allotted twenty-five minutes. For example, if the contestant called three different people and convinced all three to navigate to the website of the contestant's choosing (a flag worth twenty-five points), they would have received seventy-five points. Every attempt was made to ensure consistency in scoring for all contestants, regardless of the judge, although our scoring process does provide some subjectivity through the ability to include notes and comments for each contestant.

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 Information (OSI) was allowed to be gathered. 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, 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/social-engineer-ctf-who-is-the-deadliest-social-engineer/

Results and Analysis

As we expected, this year was an excellent competition. We continue to see improvements in the quality and preparation of the contestants. One thing we do not, see, however, are any significant improvements on the part of companies to educate and prepare themselves against social engineering attacks.

This year's competition had many similarities to previous years, but it also boasted some very exciting differences. Some changes we did notice were from the contestants. We had a higher number of unskilled and inexperienced callers this year. However, we also saw more advanced pretexts as compared to last year, indicating greater thought and preparation for the competition. We found that these contestants typically had a much better performance than those who attempted a simple "survey" or "student writing a report" pretext. Once on the phone, the well-prepared contestants who were able to stick to their storyline, commit to the path due to "inside" knowledge and get to the right person often fared much better than others, regardless of experience.

Another difference from previous years was the number of contestants that took laptops or tablet devices into the booth with them. Many of them had prepared notes or other information they could reference during the call, something that was underutilized in previous years. This may have been spurred, however, by a change in rules this year in which we required the contestants to provide call numbers to us prior to the event.

One final difference from previous years is how much more information on the target companies was found online by contestants during the OSI portion of the competition. For example, one contestant actually found an employee-only portal that allowed for a login using the credentials found in a help document. It is disheartening to note that after years of attacks and years of warnings that these valuable pieces of information are still so easily found on the Internet.

Open Source Information 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 OSI phase of the SECTF:

Google	PicasaWeb	Spokeo
Maltego	Whois	Misc
FriendFinder	WGet	YouTube
Bing	Vimeo	Foursquare
Twitter	Tineye	Friendster
PiPl	Wayback Machine	NetCraft
Bing Images	LinkedIn	Wikipedia
Facebook	Monster	MySpace
Plaxo	GlassDoor	Google Images
Google Maps	Yelp	Blogspot
Wordpress	Craigslist	Telnet
Shodan	Jigsaw	

Table 3: Commonly-Used OSI Tools

The following figure is consistent with previous years' findings, indicating that the vast majority of flags were captured during the OSI portion of the contest. The differences between OSI and live call scores are even more dramatic given that flags obtained during the OSI phase were worth half-points.

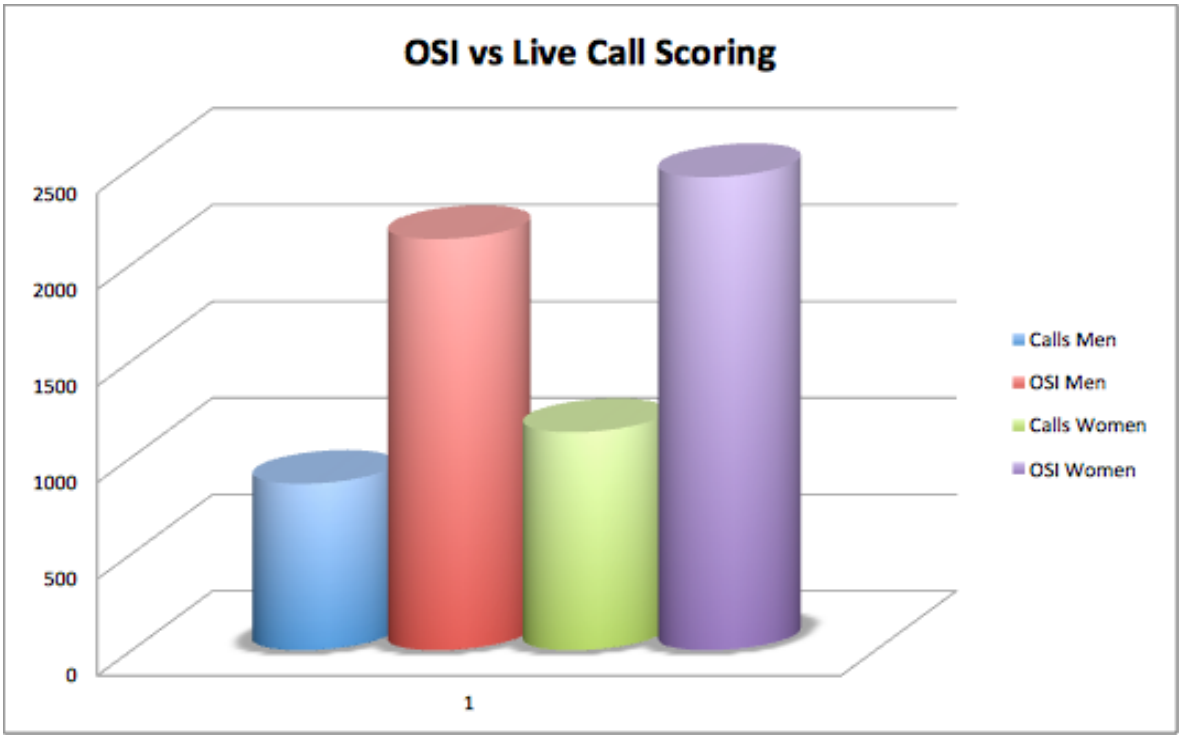

Figure 1: Comparison of Total Points, OSI vs. Live Call Phases

Figure 1 provides important insight into a few points. First, support for the 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. Second, it also stresses the issue of data leakage by organizations. Network penetration was not allowed; the flags during the OSI phase were obtained through information freely found online *without any live interaction with individuals at the target companies.* Finally, upon comparison with the live call scores by each individual (section follows), one can surmise that performance on live calls can often be affected by the skill and experience of the caller; however, it is easy to see that the amount of OSI collected, regardless of the contestant, was substantial (see Figure 2).

Figure 2 provides a side-by-side comparison of points scored by male and female contestants against their assigned company during the OSI portion of the contest. The X-axis represents the randomly paired male/female teams.

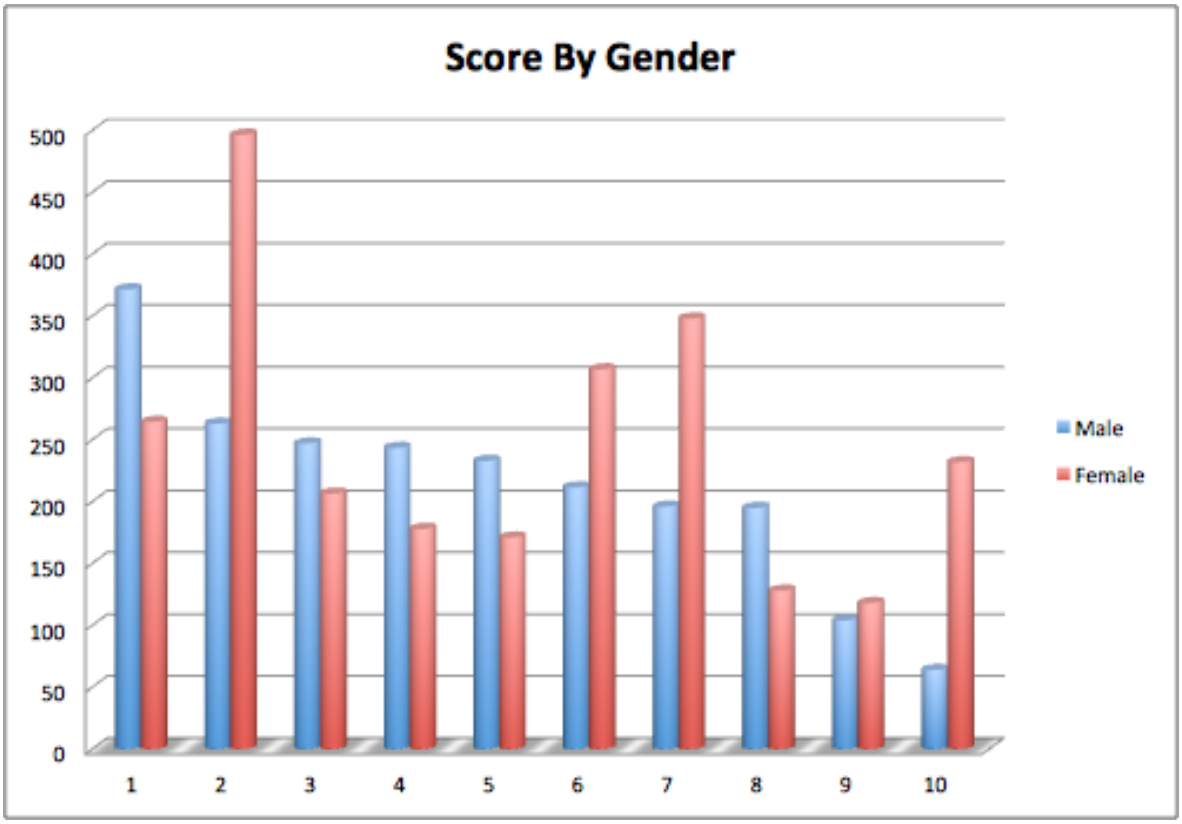

Figure 2: OSI Scores by Gender

By taking a quick glance at Figure 2, one can surmise that female performance was generally better than male, although there appears to be less consistency amongst the female contestants. This is supported by the calculations in Table 4. The mean score is simply the mathematical average of both male and female groups. The range is the highest score subtracted by the lowest score and provides information on the spread in scoring. The standard deviation is an indicator of how much the scores varied from the mathematical average; in other words, it is an indicator of score dispersion. A larger standard deviation indicates the scores are not as clustered around the average, therefore show greater variability. So with this, the numbers support what Figure 2 indicates; women, as a group outscored the men, but had greater variability in their performance. A word of caution, however, that without further analysis, it would be impossible to determine whether these differences are considered statistically significant, i.e., unlikely to have occurred through chance. Since the SECTF is not a scientific study, we will only report differences and come to realistic and logical conclusions based upon these numbers.

Mean Score for Male OSI	213
Range for Male OSI	308
Standard Deviation for Male OSI	85
Mean Score for Female OSI	245
Range for Female OSI	379
Standard Deviation for Female OSI	115

Table 4: Basic Statistics for OSI Scores

Pretexting

Again, a major difference this year was in the quality of the pretexts employed by our contestants. We saw that the vast majority of the contestants developed scenarios in which they impersonated corporate employees. This was impressive as it takes more time to prepare and more research to ensure details that might be needed are easily accessible and accurate.

In previous years, we have seen many novice contestants attempt a survey taker or student pretext. These are historically less successful than all other pretexts. We have reported that these scenarios were easy to defeat and often gave the subjects an easy way to diffuse questions. This year, as seen in Figure 3, the survey and student pretexts only consisted of 20% of those used whereas a fellow employee pretext was just over 65%.

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

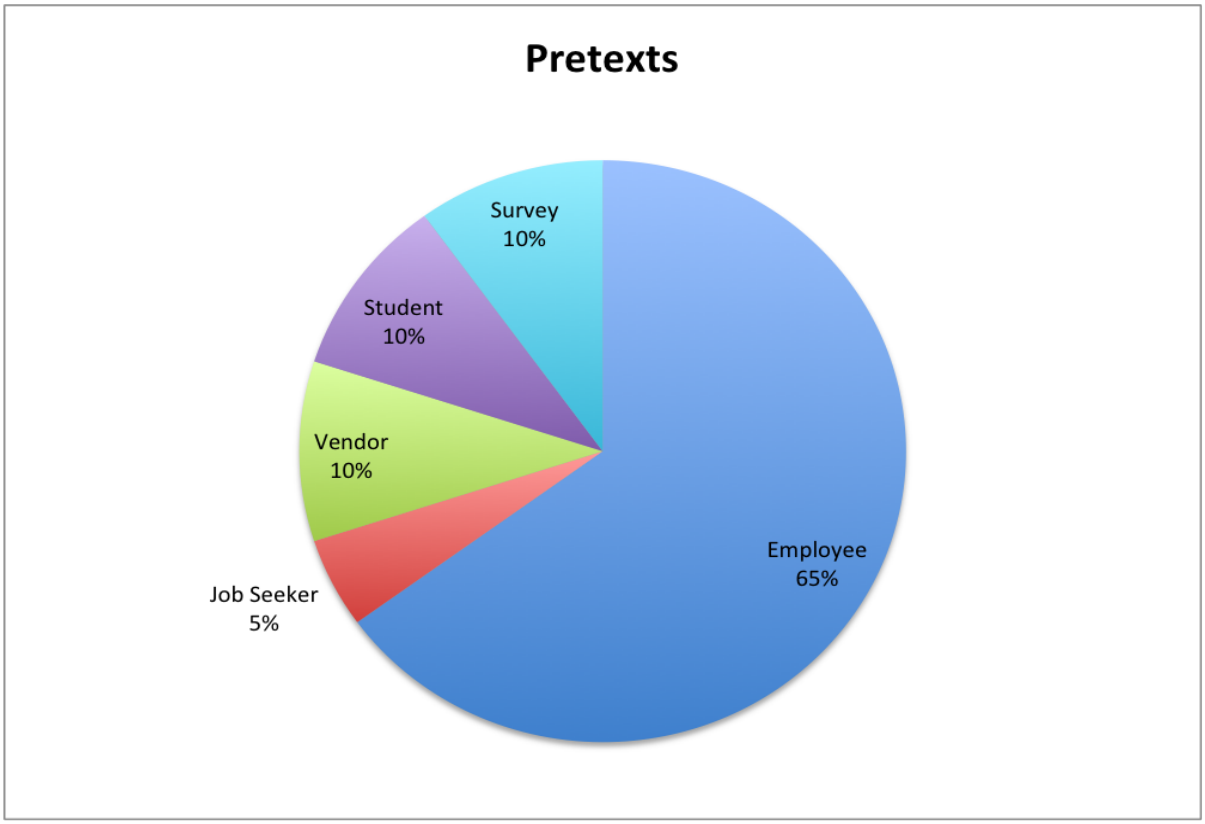

Figure 3: Pretexts Employed

As in previous years, part of our contestants' success appears to have been related to choice of pretext. Although the pretext of job seeker has worked well for us on a past social engineering penetration test, it did not have as successful of an outcome for the contestants. However, the vendor scenario worked quite well. A few contestants who were able to locate information about vendors during the OSI portion used this information effectively to pretext as an employee of a vendor company. The most successful pretext by far was that of fellow employee.

One principle that might explain why the fellow employee pretext was most successful can be found in the concept of the "tribe mentality." We inherently trust people who are part of our group or tribe. When a social engineer displays information to support that they are 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. Although to a lesser degree, this same sort of trust can also explain why the vendor pretext can be successful if done well. This concept of tribe mentality is also likely a factor in why the pretexts of survey taker or student

fail consistently as there is no initial trust and no immediate ability to build the rapport necessary for these scenarios to succeed.

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 OSI phase are not applicable. It is for that reason we congratulate all of our contestants in completing this phase of the competition.

The following figure quantifies point values scored by male and female contestants against their assigned company during the live call portion of the contest. Similar to the OSI phase of the contest, women appear to have performed better as a group, noting that two male contestants scored 0 points during this portion of the contest.

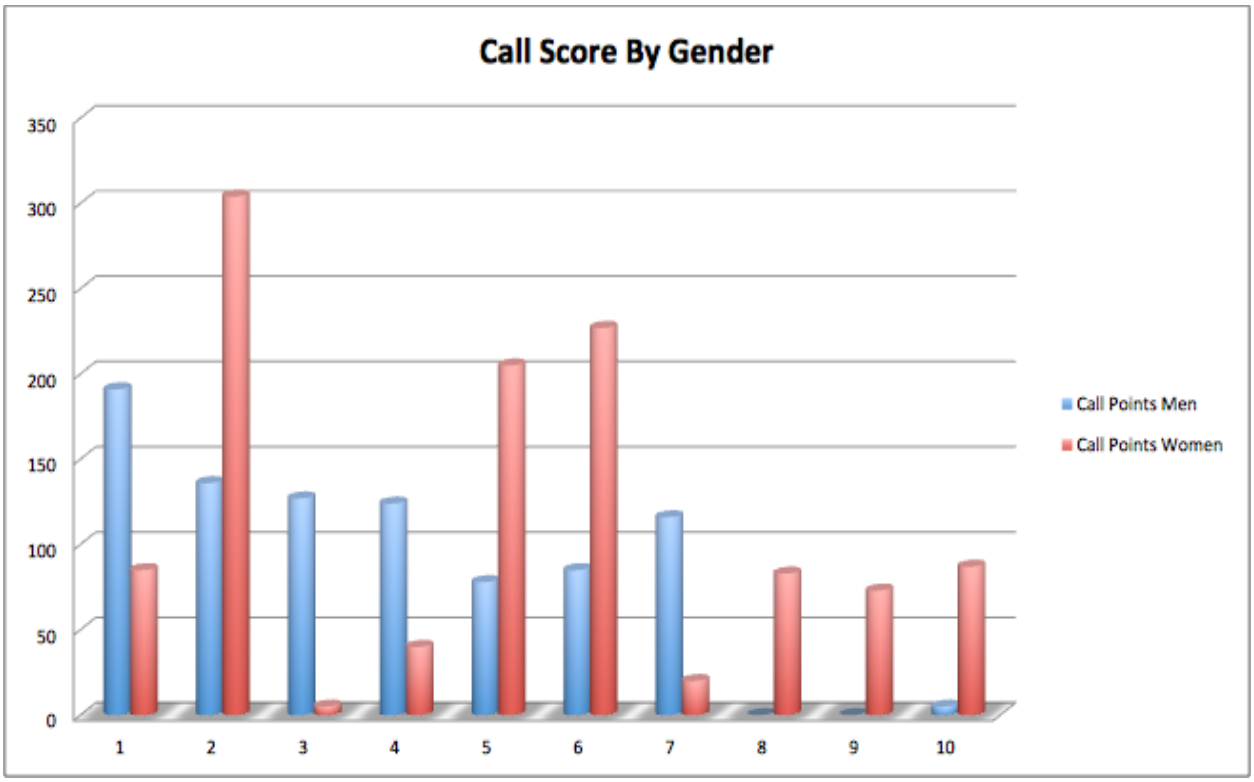

Figure 4: Live Call Scores by Gender

Calculations on the live call scores support similar differences in performance and variability between male and female contestants as the OSI portion. An interesting observation is that despite two 0 scores within the male contestant group, women still had greater variability in their group as indicated by a much higher range and larger standard deviation. This would be explained by viewing Figure 4 and noting that there is a very large drop-off in scoring within the female group after the top three scores while the male scores stay within a smaller, more consistent, range.

Mean Score for Male Calls	86
Range for Male Calls	191
Standard Deviation for Male Calls	66
Mean Score for Female Calls	113
Range for Female Calls	299
Standard Deviation for Female Calls	99

Table 5: Basic Statistics for Live Call Scores

The following figures are an interesting observation regarding the gender of the contestant versus the gender of the person reached at the target company. The ratios for the contestant groups are almost directly opposed to one another. Combining this and overall performance, we can observe that within this small dataset, women callers appear to have performed better against male targets than vice versa. While this difference may be due to chance or other unknown factors, it is at least a trend that will be interesting to follow in future competitions. Research findings in the area of gender and helping behavior suggest a complex relationship amongst factors such as social roles, type of help, risk involved, etc.

Figure 5: Male Contestants vs. Gender of Target Company

Figure 6: Female Contestants vs. Gender of Target Company

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 side-by-side comparison of total scores (combination of OSI and live call phases) by gender.

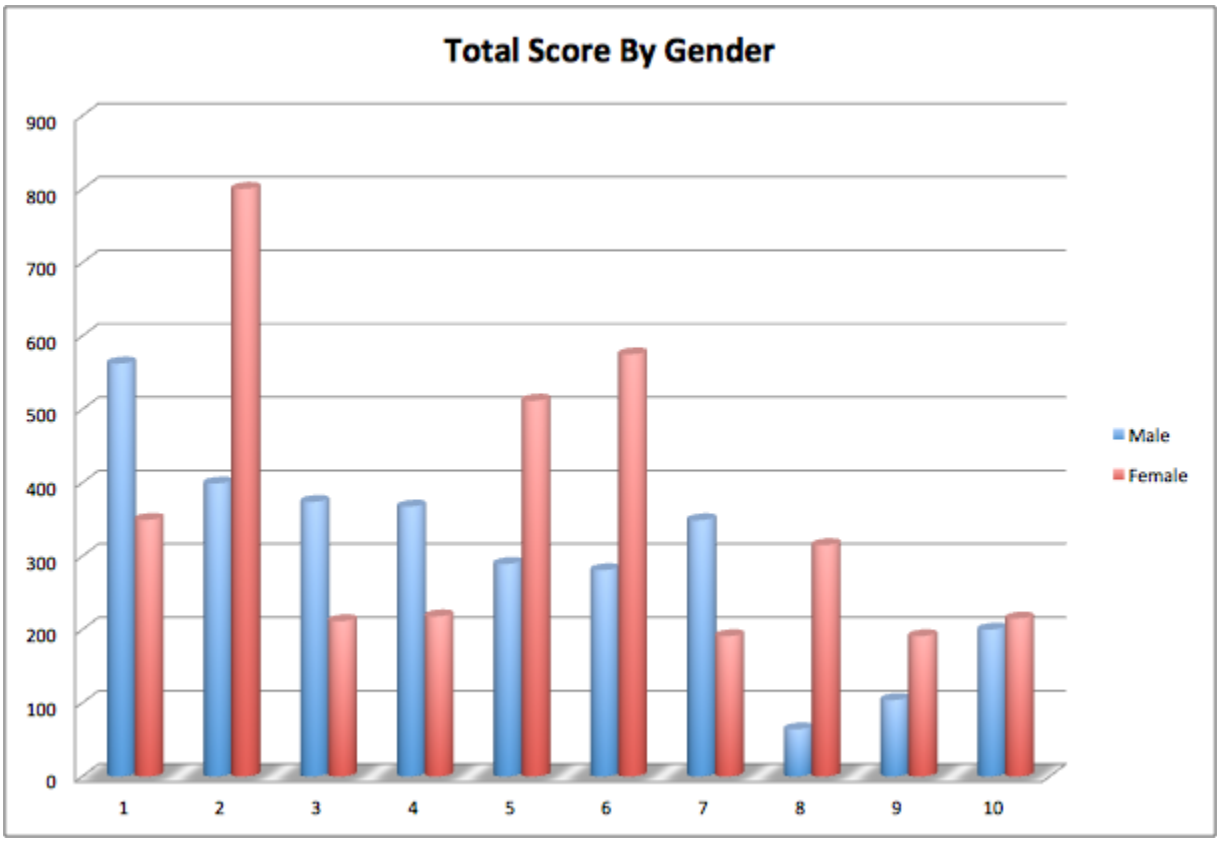

Figure 7: Side-by-Side Comparison of Male/Female Scores

When compared side-by-side, we see that women placed in 3 of the top 5 scores. In addition, their group score average exceeded the male scores by approximately 30 points in both the OSI and live call portions of the contest and their total score difference was close to 600 points. Based on these indicators, we concluded that the women were victorious as a team this year. The interesting variability in their scores may be hypothesized from the fact that they were an extremely diverse group, coming from very different backgrounds and different experience levels. It should also be noted that one of the original female contestants was a no-show, and a female audience member who was given 20 minutes with the original contestant's OSI report

for preparation took her place. Although her performance was admirable, this lack of prep time may have added to the high variability of the female group. Although we ensured diversity as a group, the men tended to be more homogenous in background and experience level and perhaps this is was reflected in the smaller range of scores.

Attendees to DEF CON know that we announced both our first and second place winners as female. In the interest of full disclosure, the second place top scorer was actually male (please see Figure 7). However, upon review by the judging panel, this contestant was disqualified. Our rule set and philosophy as an organization are that there would be no methodology employed that made the target feel at risk in any way. Although we have a full understanding that malicious individuals will utilize unethical and manipulative tactics, our practice is entirely based on education, not punishment, as a way to change behavior. The contestant in question threatened the employee with termination as well as being responsible for the loss of a major negotiation if she did not comply in order to manipulate her into providing the flags. The judging panels made a unanimous decision that this was unethical conduct, eliminating this contestant from consideration.

Aside from the contestants, 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.

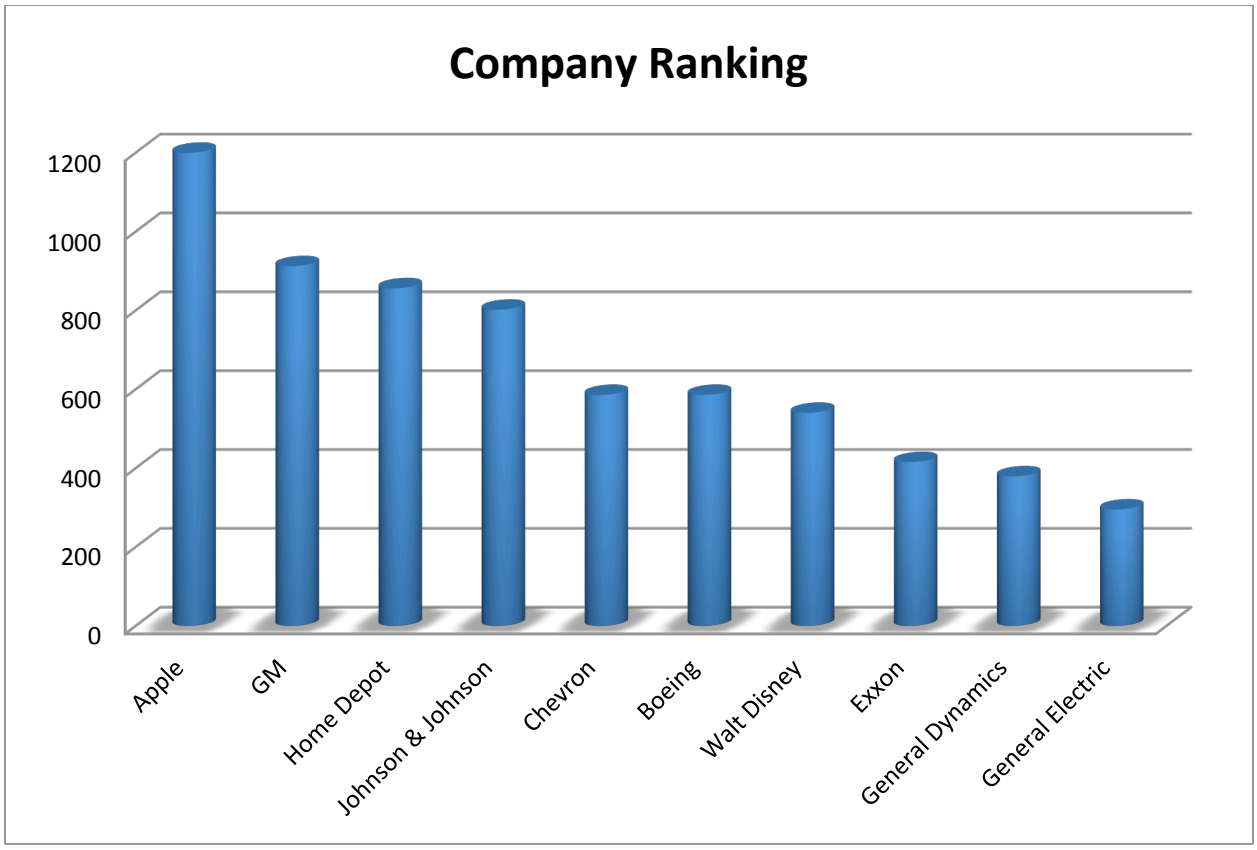

Figure 8: 2013 SECTF Target Company Performance

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.*

Finally, Figure 9 illustrates the number of times each flag was obtained during both OSI and live call phases. At a glance one can see that the top two most commonly obtained flags were browser and OS. With these two pieces of information, the simplest way to breach network security would be through a specific phish containing links that would either release malware or lead the target into clicking to a malicious website targeting specific browser/OS vulnerabilities. In addition, the flags captured during the OSI phase would be highly useful in the development of strong pretexts, e.g., posing as a member of the janitorial staff to gain entry into an office and collect information that may have been improperly disposed of. It is interesting to note that ALL flags were surrendered by the targets at least once.

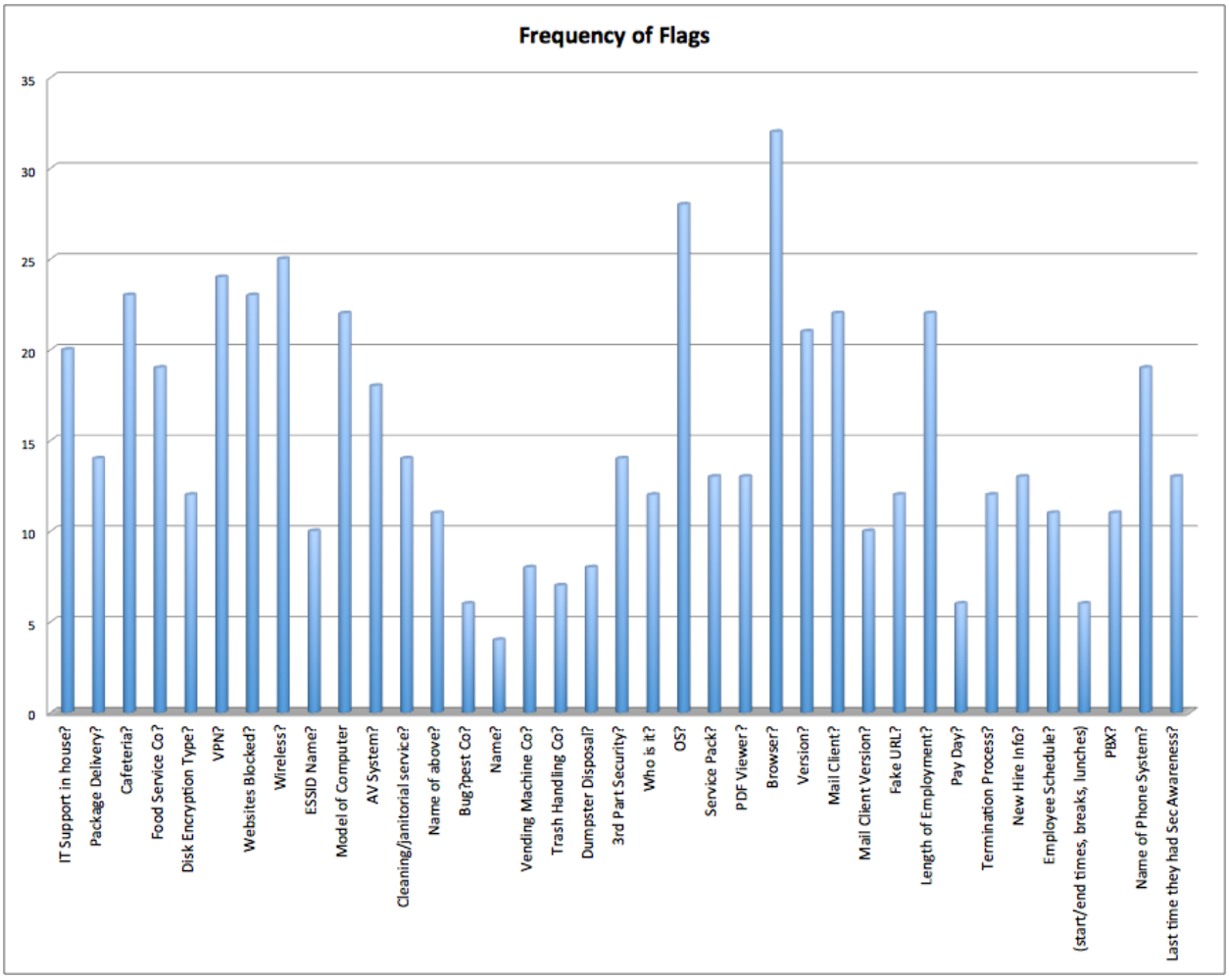

Figure 9: Frequency of Flags

Discussion

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, and in that time, despite numerous high-profile security breaches in the commercial sector, we have not seen consistent improvements that directly address the human factor for organizations. Second, most companies still maintain potentially damaging amounts of information in freely accessible locations online. Companies must balance security with the open communication necessary to run the business. However, more emphasis needs to be placed on critical thinking in the determination of what is released in a public environment.

Third, the malicious social engineer does not necessarily need exceptional skill or expertise to be successful, simply good planning and the ability to conduct thorough research on their targets. Our winner this year is not a professional social engineer and surpassed the next competitor by over 200 total points. She conducted an exceptional amount of research on her target, developed an excellent pretext, and was fully prepared prior to the contest.

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. Corporate Information Handling and Social Media Policies

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.

Guidelines, policies, and education can help the employees understand the risks associated with information exchange in both their personal and professional lives.

2. Consistent, Real World Education

One of the areas that appear to be lacking across the board is quality, meaningful, security awareness education. In our experience, there is a definite relationship between companies that provide frequent 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 consistent, frequent and personal. It doesn't require that a company needs to plan 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.

3. Regular Risk Assessment and Penetration Test

One of the most necessary aspects of security is the social engineering *risk assessment* and *penetration test*. When a proper social engineering risk assessment is conducted, areas where a company is vulnerable to attack 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.

These are just three of the many strategies that can be utilized to help 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.

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

www.social-engineer.com

www.wombatsecurity.com

www.pindropsecurity.com