Social-Engineer.org

Social Engineering Capture the Flag Results

Defcon 19

defcon@social-engineer.org

Written by:
Christopher J. Hadnagy
& James O'Gorman
Researchers: Dan Sharp & Eric Maxwell

Table of Contents

Executive Summary

Defcon 19 marked the second year that the Social Engineering Capture the Flag event took place. Dubbed "Social Engineering CTF - The Schmooze Strikes Back", the event built on the first year's success by expanding the number of companies called, the requirements for the contestants, and the flags that were sought after.

In approaching the organization of this second year, we wanted to attempt to answer some questions that we were left with after Defcon 18's SE Capture the Flag event. The first question being, is there any difference between two companies in the same industry regarding defenses against social engineering attacks? Second, what techniques were effective in eliciting information from companies and why? Finally, what defenses were effective in preventing the leakage of information from companies in the course of the contest?

Last year's event had the goal of raising awareness of how social engineering could be a threat to companies as well as exposing each company's vulnerabilities. The contest was a demonstration of the type of attacks social engineering employs in general, as well as commonly used tactics that social engineers employ. When the event concluded, a report was generated showcasing the plethora of information gathered by each contestant, including extracted company information, which could then be used to facilitate an attack. The multiple high profile hacks that occurred in the summer of 2011 (HB Gary, etc.) were all facilitated by social engineering attacks, validating the conclusions that our report produced after last year. The focus of this year's report has been to reflect the overall goals of the Capture the Flag competition. The report focuses on the social engineering techniques utilized by each contestant as well as the reasons behind why each technique succeeded or failed.
The competition drew a wide range of contestants, from skilled social engineers to unskilled enthusiasts. Each contestant took part in a wide array of research, which included initial info gathering, attack vector development, and a twenty-five minute social engineering phone call placed to his or her assigned target.

Primary Findings

As previously mentioned, the goal of this year's report is to showcase the techniques used and to demonstrate why they were or were not successful. Industries represented this year included retail, airlines, food service, technology, and mobile services. By comparing a cross section of companies from multiple industries, an accurate view of the state of social engineering effectivness was obtained. Listed below are the basic statistics of the Capture the Flag contest.

Number of Companies Called:	**14**
Possible Flags:	**62**
Number of Companies with Flags Captured:	**14**
Days Contest Was Held:	**2**
Companies Who Put Up Resistance:	**4**
Employees Who Put Up Resistance:	**3**

The point values listed above do not always indicate a company's true weakness or strength. The "X factor" is the skill of the caller and the employee they get on the phone. In this report we we will use data collected during the live call to determine the way the companies handled the social engineering attack.

The companies that callers had the most difficulty extracting data from were retail-based companies. Companies like AT&T Stores, Walmart, and those that dealt with customers in retail settings tended to be more cautious and reluctant to answer questions and inquiries. Companies that had large call centers or customer support representatives such as the Airlines Industry, Tech Industries, and other such companies seemed to be the weakest. Therefore, we can conclude by the calls that security awareness training is less prevalant and less effective in customer service areas as opposed to retail settings.

Another preliminary finding was that in all cases where the caller asked the target to visit a URL, even in the cases where there was some relucatance, the target ended up visiting the URL. The following pages will outline this in greater detail.

Background and History of CTF Event

The team at Social-Engineer.org was invited to run the Social Engineering Capture the Flag (SE-CTF) event for Defcon 19. The core ground rules of the competition remained the same as in the previous year, including not collecting sensitive information such as credit card information, social security information, or passwords. Like last year, we also avoided sensitive industries such as Government, Education, and Finance. Unlike last year, this year's announcements were met with surprising support from corporations and the media. What didn't change was the amazing support from the community.

At the start of the contest contestants were assigned a target company. Each contestant was given two weeks to use passive information gathering techniques to build a profile report on their target company. No direct contact between the contestant and the target was allowed during the information-gathering phase. The information was then compiled into a dossier that was turned in and graded as the contestant's score. This year each contestant was given a sample of a professionally written social engineer report as well as a template for him or her to use in writing the report.

There were three ways contestants could score points during this competition. This year, half points were awarded for any flag captured during the initial information-gathering phase of the contest. Contestants were able to obtain many of the flags through this initial phase. The second phase of the contest took place during DefCon 19. Contestants were allowed 25 minutes to call their target and collect as many flags as possible for full points. Finally, points were awarded for the style and professionalism of the report.

Flags

The flags were pieces of information based on non-sensitive data pertaining to the inner workings of a company. Each flag was given a point value based on the degree of difficulty in obtaining the information. The contestant's job was to develop a believable pretext along with a real world attack vector that wound enable them to obtain as many flags as possible. The attack was then performed live at Defcon 19 during their 25-minute time slot.

Logistics		**Company Wide Tech**
Is IT Support handled in house or outsourced?		What operating system is in use?
Obtain information about the badges used		What service pack/Version?
Who do they use for delivering packages?		What program do they use to open PDF documents & what version?
What time do deliveries occur?		What browser do they use?
Do you have a cafeteria?		What version of that browser?
Who does the food service?		What mail client is used?
Who does offsite backup?		What version of the mail client?
Bonus points for identification of pick up dates		Fake URL(getting the target to go to a URL)
Do they have offsite back up?		Can they view flash content?
How is document disposal handled?		Ports open outbound?
Do you use any kind of authentication token with your passwords?		Do they have an intranet?
Do you use disk encryption? If so which type?		Any password construction limitations?
Other Tech		**Employee Specific Info**
Is there a company VPN?		How long have they worked for the company?
What vpn software		What days of the month do they get paid?
Do you block websites? (Facebook, Ebay, etc)		Employee termination process?
Is wireless in use on site? ESSID Name?		New hire orientation information?
What make and model of computer do they use?		Employees schedule information - (start/end times, breaks, lunches)
What anti-virus system is used?		
Do you use a key fob with a rotating number?		Do they have a PBX system?
What mobile devices are used?		What sort of phone system is used?
Are there public terminals open for use?		When was the last time they had awareness training?
Is there network access in the conference rooms?		
Can Be Used for Onsite Pretext		
Where do they get copier paper?		Bonus points for identification of pick up dates
What toner vendor is used?		What time does the building open/close for the day?
Do you have a cleaning/janitorial service?		Is there video surveillance of the location?
What is the name of the cleaning/janitorial service?		Is the building protected by security systems at all?
Do you have an bug/pest extermination contract		Do you have a 3rd party security guard company?
With Whom?		Who is it?
What is the name of the company responsible for the vending machines onsite?		
Do they have trash handling?		
Who handles their trash/dumpster disposal?		

Results and Analysis

Companies Called

The fourteen target companies this year were:

1. Apple
2. AT&T
3. Conagra Foods
4. Dell
5. Delta Airlines
6. IBM
7. McDonalds
8. Oracle
9. Symantec
10. Sysco Foods
11. Target
12. United Airlines
13. Verizon
14. Walmart

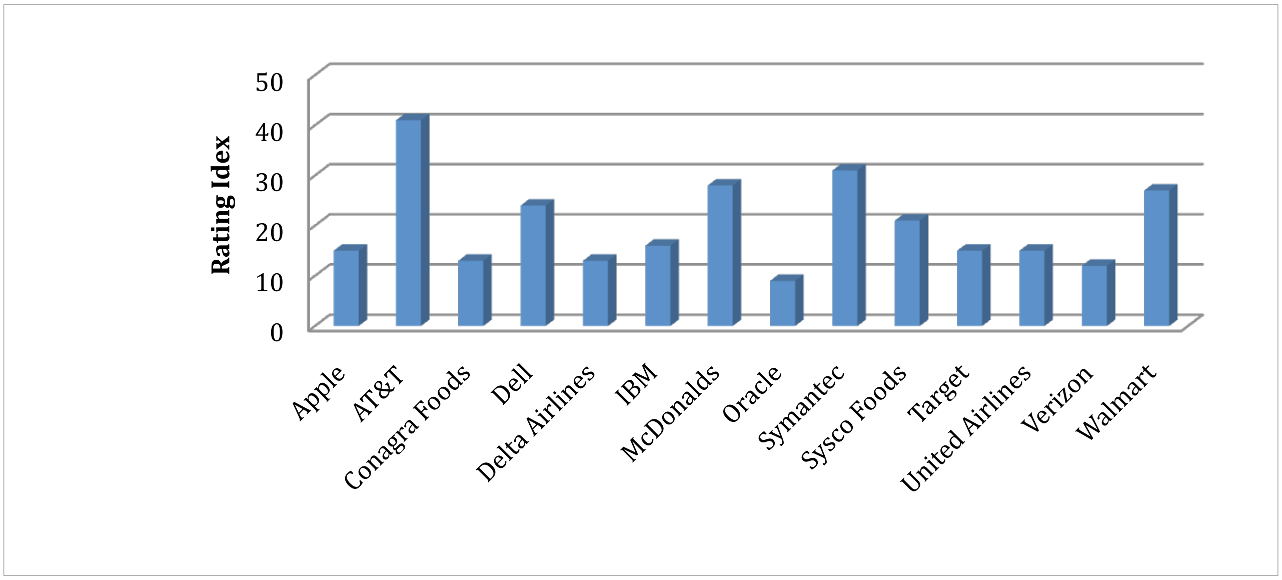
Target Ranking

This year it was decided to rank each target based on the following set of criteria.

- Online Score (how much information is released online)
- Number of flags obtained
- Resistance to social engineering attempts
- Observed in person – this score is how we felt as a team of social engineers listening to the call as to the state of this companies security
- Visited URL when asked

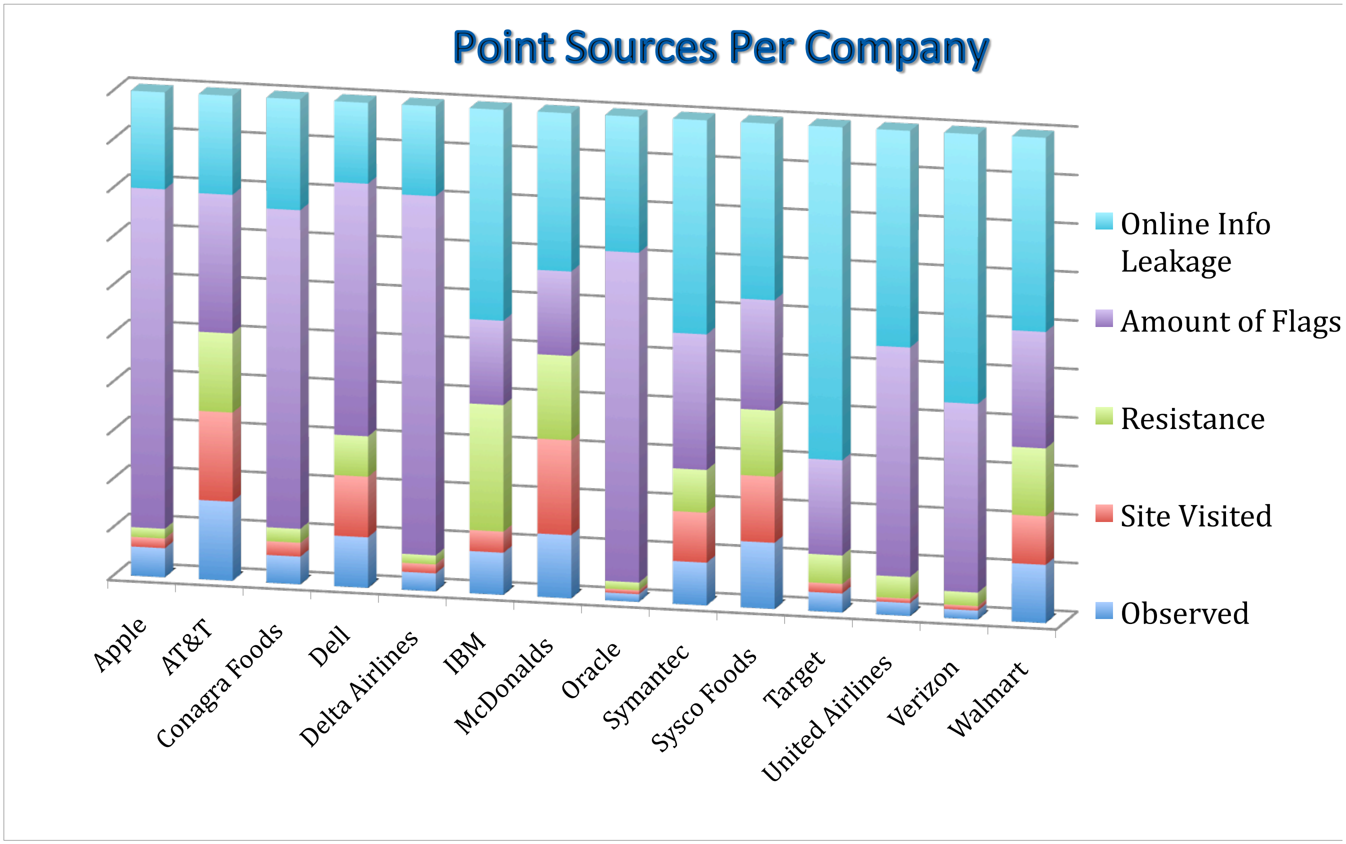
The highest score a company can get is 50. A ranking of 50 would indicate that this company has proven a resistance to social engineering and they have an online presence that is not leaking information or that the information found would make it more difficult for a social engineer to develop usable attack vectors.

A lower score indicated that a company was more vulnerable to a social engineering attack.



The chart above shows some startling statistics. Every company was susceptible to a social engineering attack with very little effort by a potential attacker.

For a company breakdown on each target company see below:



In the above chart, the top light blue bar indicates online leakage and this shows the amount of data that was leaked through passive information gathering. In other words, the larger the section, the more information that was found. Also in the above chart, the "Amount of flags" section indicates the amount of flags the company gave up during the contestants call.

"Resistance" indicates how much push back the attacker received from the company during the call. The larger the green bar, the more a company resisted revealing company information. The "Sites visited" bar indicates the attacker's ability to trick the company into visiting a URL provided by the attacker. "The observed" is based on our professional observation during the attack. The better the company did, the larger the blue area you see.

Dossiers

Each contestant was given two weeks to perform passive information gathering on his or her target using Open Source Information (OSI). The objective was for the contestant to create a professional dossier the same way a professional social engineer would when entering a professional engagement. To give each contestant an advantage we provided a sample social engineer penetration testing report and template to use during their report writing session.

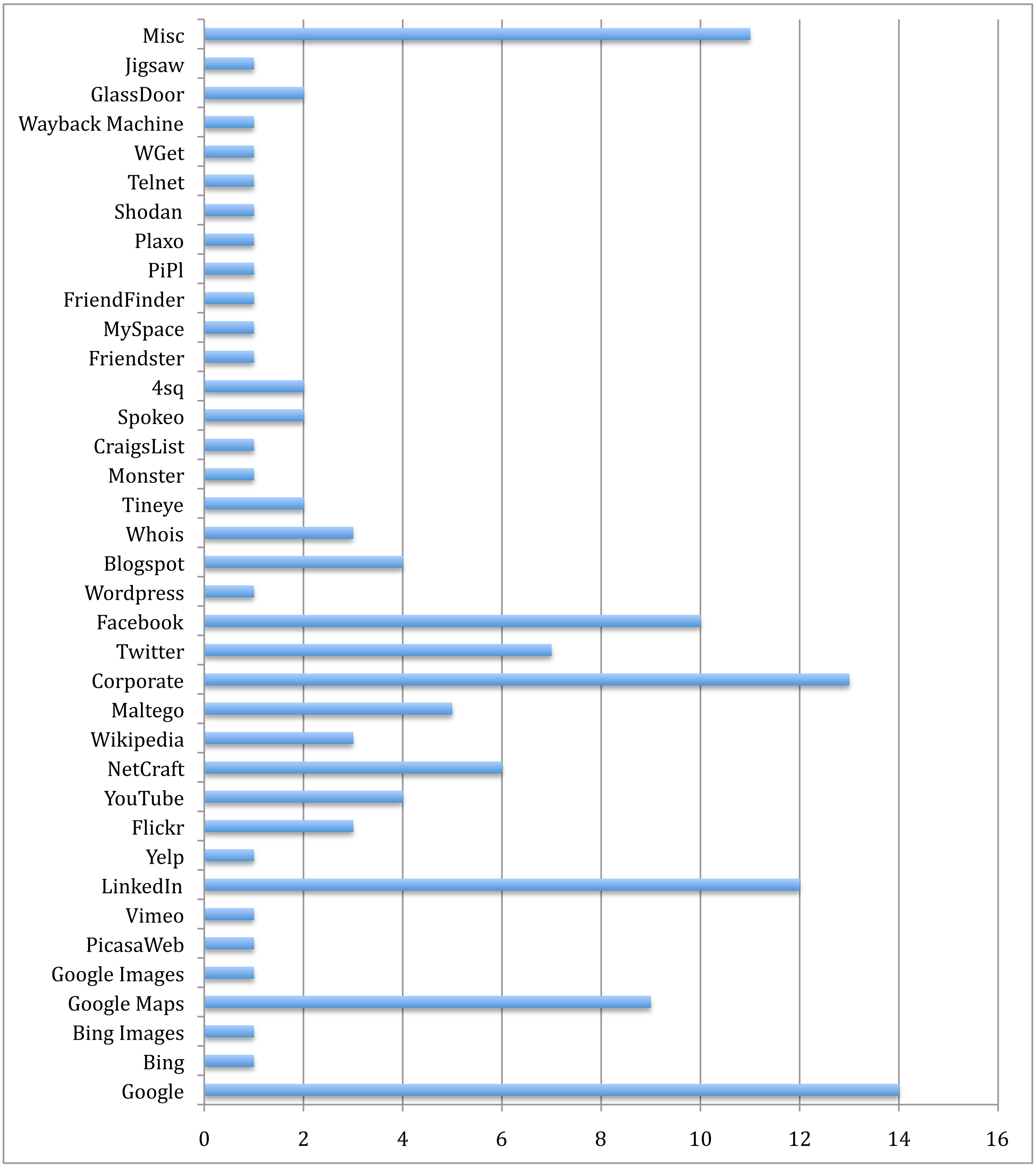
Information Sources

The contestants used many different sources for gathering data on the assigned targets, with a few sources used by almost every contestant, including: Google, LinkedIn, Facebook and Maltego.

This list represents the different methods of information gathering the contestants used.

Google	Maltego	FriendFinder
Bing	Twitter	PiPl
Bing Images	Facebook	Plaxo
Google Maps	Wordpress	Shodan
Google Images	Blogspot	Telnet
PicasaWeb	Whois	WGet
Vimeo	Tineye	Wayback Machine
LinkedIn	Monster	GlassDoor
Yelp	Craigslist	Jigsaw
Flickr	Spokeo	Misc
YouTube	4sq.com	Friendster
NetCraft	Wikipedia	MySpace

The chart below shows how many times each of the information sources was used.


Misc
Jigsaw
GlassDoor
Wayback Machine
WGet
Telnet
Shodan
Plaxo
PiPl
FriendFinder
MySpace
Friendster
4sq
Spokeo
CraigsList
Monster
Tineye
Whois
Blogspot
Wordpress
Facebook
Twitter
Corporate
Maltego
Wikipedia
NetCraft
YouTube
Flickr
Yelp
LinkedIn
Vimeo
PicasaWeb
Google Images
Google Maps
Bing Images
Bing
Google
0
2
4
6
8
10
12
14
16

The content a company chooses to put on its website proves to be critical to overall security. This is not something that should be handed off to a company's marketing department and forgotten about. Regular review of published content should be conducted. Companies must understand that just because content is not linked, does not mean it will not be discovered.

This year again showed the importance of LinkedIn from a corporate security perspective and showed an increase in usage of Facebook over last year. Information leakage via social media is a difficult problem to solve due to how it is used and the frequency it is used in today's society. Having access to social media from computers and cell phones means that people can update their accounts instantaneously, from anywhere. The ease of which an employee can share data can contribute heavily to information leakage.

The contestants were only allowed to use passive information gathering techniques leveraging Open Source Information from the sites and tools listed above. None of the contestants were allowed to port scan, visit the company's physical location, call, email, or contact the company or its employees in any way. Considering that passive information gathering was the only info gathering allowed, the information found was shocking.

The information below will show potential threats with only passive information gathering as the source:

Personal Blogs

Information: An employee of one company blogged about very specific IT procedures involving what social media sites were allowed and which ones were blocked. This employee then went on to describe how IT procedures were circumvented. This information should not be posted on the Internet.

Vector: Finding this information would allow a social engineer the ability to know allowed sites, ports and emails to spoof. For example if social media site MySpace is allowed, the attacker can spoof emails from that site.

Mitigation: Employees should be bound by Non Disclosure Agreement (NDA) to prevent this type of information leakage. Security staff should scrape the Internet for offenders and take action. Awareness of an organization's online presence goes far beyond content that is owned and controlled by the company.

Information Leaked Via Corporate Website

Information: One company indexed all of their employee information on their website, making searching for complete company info a breeze. They indexed employee names, titles, email addresses, phone numbers, and even cell phones. This company also publicly disclosed their media disposal policies and practices. Finally this same company published a PDFmanual containing their entire security plan. Every step of their security procedures was outlined for everyone to read and analyze.

Vector: A potential attacker would be able to outline a very detailed attack. They would know when and how hard drives and sensitive data is disposed of, allowing for interception. In addition, having the entire security plan allows for an attacker to find the weaknesses without having to go onsite and risk the potential of being caught to identify the weaknesses.

Mitigation: Giving this much information to the public is not necessary and should be avoided by not indexing sensitive corporate data. Knowing when and how hard drives and sensitive data are handled can allow the attacker to intercept the disposed data. This data needs to be removed from the corporate website and greater care needs to be taken to not allow for release of these types of data.

Company Search and too much freedom

Information: Another company had a handy search screen, which located an employee's phone number, email address (a very serious social engineering tool) and also an open anonymous ftp server. We assume this was for document dropping, as there was much content left on this open and free FTP server. The same company's employees had a very large and public presence across all social networking sites as well as heavy use of Location Based services such as Foursquare. This allows an attacker to keep very easy tabs on the locations of employees. Employees were diligent about updating their social media and blog sites with information that pertained to their work, role, personal interests and hobbies.

Vector: Besides the obvious vector where an attacker could locate employees on the website and all their contact info, the FTP server could allow for uploading of malicious software. The heavy usage of social media sites allows an attacker to find usable vectors based on hobbies and target the right person in the right part of the company for maximum effect.

Mitigation: We recommend strict social media guidelines be put into place that prevents the employee from mixing social and professional data. In addition, continual education on the dangers of phishing, scams and social engineering could help employees balance what they allow out on the web.

Vendor Information Leakage

Information: One company used dozens, if not hundreds of vendors. Each project they were involved in was spoken about in extensive detail by these vendors. Not only did they outline many projects they had going on, but the specific employees and vendors involved as well as specific engineers involved. Vendors were found to discuss in great detail the technology and other aspects of the projects they were involved in on their sites.

Vector: A social engineer could use this data to spoof as one of the vendors. With detailed information on projects, it would be much easier to pretext as one of the vendors and gain trust and build rapport due to that knowledge.

Mitigation: This is a particularly hard one to mitigate. It might require that a company keeps a list of allowed engineers and anyone who calls from a "vendor" must be verified before information is given.

Badges and Confidentiality Breached

Information: One company's employees posted very clear pictures to the Internet containing pictures of their employee badges. The pictures not only showed their badge design, but their names and position were clearly visible. A large sample of this company's employees had extremely detailed personal information readily available. This information included names, phone numbers, relatives, addresses, etc. During research, a number of confidential documents were discovered through a simple Google search. A search for "[company] confidential" revealed 61 pages of documents marked confidential, some of which were tagged "[company] Confidential - Highly Restricted."

Vector: Of course the obvious is an onsite attack where an employee badge would be very easy to reproduce with little effort and low cost. The document that was marked confidential leaked very sensitive data that would give an attacker the information needed to launch many full-scale attacks.

Mitigation: The mitigations here are obvious but need to be stated. Employees need regulations within their companies regarding how much information they are allowed to release on the web, especially information that can identify company property or badges. In addition, any document that needs to be marked as "confidential" should be protected with a high degree of vigilance and skill.

Work Orders Lead to Breach

Information: In one instance the contestant found employee resumes posted on the Internet containing specific technical details and configurations. Employee names were embedded into PDF documents and posted online. Server names and printer paths were also exposed. In addition, a massive 60-page document was discovered online for this organization, which revealed several key pieces of sensitive data such as samples of work orders, logins with username/password combinations and API documentation.

Vector: Knowing this much detail about a company and their infrastructure will enable the social engineer to know exactly where and how to attack the organization. Knowing the username and password combination of employees, of course, opens up direct attacks upon the company.

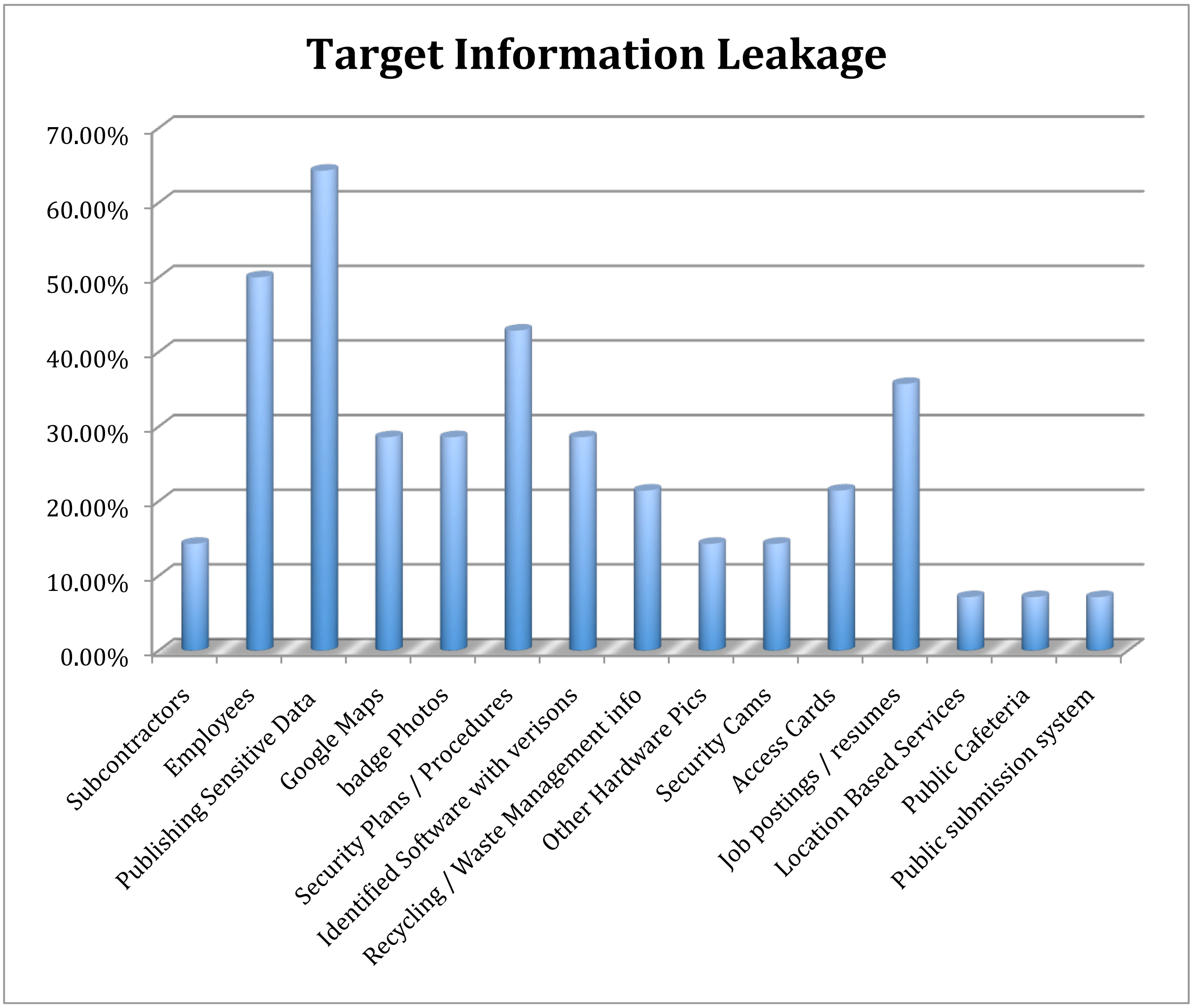
Mitigation: Again, the mitigation is more vigilance in protecting sensitive data, as well as corporate policies that give employees rules of how to conduct themselves with documentation. Cleaning out metadata from documents that will be posted on the web is also very important.

Plethora of Documents

Information: One company had a lot of its sensitive information revealed from pictures that employees and fans had posted on internet sites such as Flickr.com. By scanning photos taken, we can clearly see badge design, operating systems in use, browsers in use, lanyard design, CCTV locations, RFID scanners, company vehicles, and sanitation companies used. Many resumes were also an issue for some companies because many were found online, posted by current and former engineers. They clearly outlined specific technologies used.

Vector: The release of personal and company data opens the doors wide open. Knowing not just the technologies used but also what kind of a job a person is looking for can give an attacker a many usable vectors to collect all sorts of personal data as well as drive targets to malicious sites and/or files.

All the targets displayed varying levels of information leakage. Below is a graph that outlines the percentage of companies that leaked different types of information.

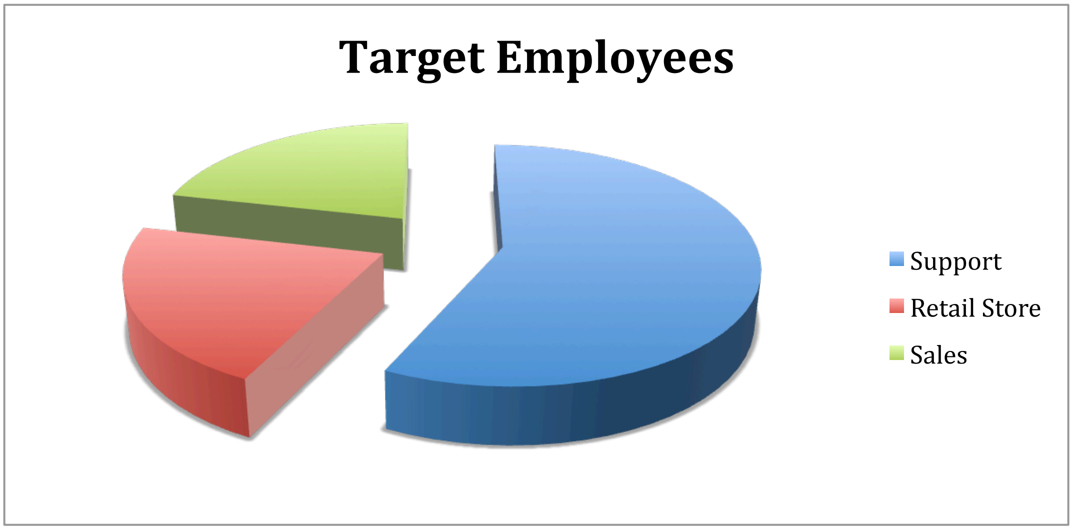


With close to 70% of the companies leaking some form of sensitive data, it is not too harsh to say that full-scale social engineering attacks could be launched with little more than the passive information that was gathered by the social engineers.

Calls

Targeted Employees

This section outlines the areas within the target companies that were used in the various calls. These areas could be broken down into three main sections: support / customer service, retails location, or a sales office.



Support and Customer Service took the largest number of calls. This was the most used area due to the ease of obtaining information through these channels. Customer Service representatives are normally trained to be helpful. The "customer is always right" type of attitude was prevalent and the employees seemed to field a lot of questions.

Additionally, many companies will tend not to invest in much awareness training for high turnover positions. While the logic behind that is understandable, that decision should be supported by limiting the amount of information possessed by the employee in that job and limiting the overall actions that can be taken by these high turnover employees.

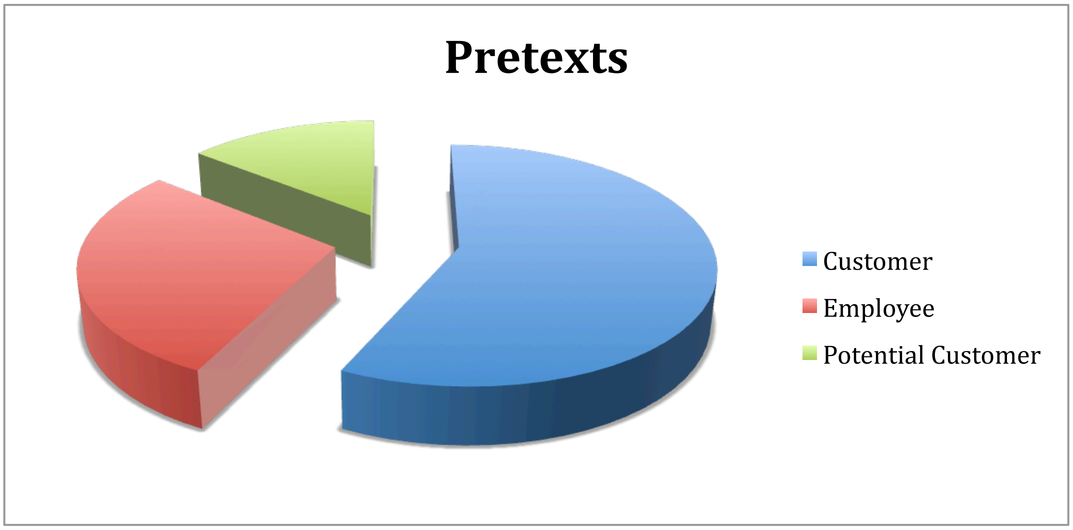
Pretexts Used

The pretexts used can be broken down into three main categories – Customers, Potential Customers and Employees.

The largest number fell under customers, as this pretext allows for a broader range of questions and conversation. It is easy to use and most companies in this economy want to please customers to retain them and therefore are more willing to deal with odd questions.

The Potential Customer pretext is also very effective because most companies want to make potential customers feel special and entice them to come aboard. Giving out little tidbits of information doesn't feel bad or appear as a security risk.

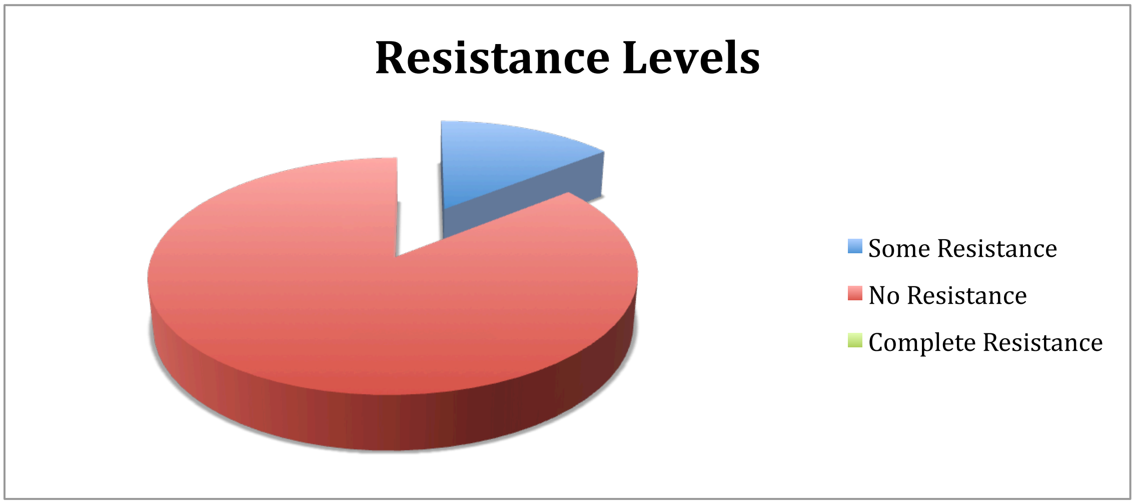
The hardest pretext, but also the most effective when performed correctly, is the fellow employee. A fellow employee is giving certain information without even asking, is allowed into the "inner circle", and is freely spoken to because of inherent trust. We saw this pretext used more than the potential customer one, which was surprising due to its difficulty level, but in each case it was used to obtain large amounts of data.



In an actual Social Engineering penetration test, the pretext may be more complex and need more time to build. The contestants are only given 25 minutes to state, build, and make their pretexts believable. For that reason the pretexts tend to be simpler. In addition, we did not allow any onsite social engineering, so common pretexts of delivery people, service people, or support representatives are not applicable to this contest.

Defenses

One of the most important parts of this report is, of course, the level of resistance targets display to social engineering attempts, and their ability to perceive social engineering attempts. In addition to the level of resistance, we try to ascertain why there was resistance and use that data to determine how effective it would be to combat a targeted social engineering attack. We collected this data by combining what we heard and saw during the Capture the Flag event as well the amount of calls with resistance a social engineer had.



As the chart shows there was absolutely no company that completely resisted, and only a small fraction showed any resistance at all.

Those who did show resistance did so in only a very small number of ways:

Website Blocking Software

In only a couple of cases did the target state that they tried to go to a URL and could not pull it up due to being blocked. Although this method did save the target from opening a URL, the fact is, the employee still tried to visit the URL, showing a willingness to comply. This willingness to comply could be exploited by a social engineer to get compliance on other actions that could cause a serious breach. In addition, all the employees that tried and were blocked complied with other requests.

This is an interesting concept due to the politics that are involved.. Often times blocking access to random sites is seen as negative and bad for company morale. However, the question must be asked: What web sites are actually required for business purposes? While this is not an easy question to answer, the benefit that would be gained deploying systems that are engineered to simply accomplish company goals and nothing else is obvious. While costs are higher up front, money is saved in the long run by decreased repair (less happening, less to break), decreased costs, and increased productivity. The wide spread adoption of smart phones have, in many cases, provided employees with an outlet for personal internet use removing the burden of carrying that traffic on company networks.

Security Awareness

In a few cases the question was presented as to the level and frequency of security awareness training at the target company. In a couple cases the target stated they had frequent security awareness training at their company. Even though that may be the case, the target, or another person at the company, answered all the requests.

On the surface, this draws into question the effectiveness of awareness training. If these targets are receiving training already, and there is no noticeable benefit in terms of increased security, the conclusion is that the training being provided is not worth the money being spent. However, the issue is more complex then that. While it is certainly the case that better engineered systems that make it hard for users to do the wrong thing would provide benefit, we know that is not enough. A well-trained and educated human is worth far more than any automated system in terms of actual defense.

It is recommended that companies review the structure of the awareness training programs and how they are actually built. Far too often we have encountered companies whose solution to awareness training has been simply purchasing a video package off the shelf that all employees must review on an annual basis. If we are honest with ourselves, we know that what should be "training" becomes nothing more then a tolerated nuisance that employees get through as quick as possible, with as little attention paid as possible.

For awareness training to be effective it must focus on the employees real job, in real situation that they may encounter. When a contestant delivered a pretext to an employee at a target company, the employee would have had a spark of memory from when they had encountered this same, or similar, situation in their training program. That spark of memory would have been a clear indicator that something was wrong with this call and care would be taken.

Lack of Knowledge

This particular protection method, although mildly effective, is not really a method that should be promoted. In a few cases the employee's lack of knowledge into certain technological areas barred the caller from getting the information they attempted. Again, this is not a method we promote as being good, but it is something that should be considered as it did protect a very small amount of data from being released.

In many respects this was an implementation of “need to know” applied in an unintentional basis. The risk posed by deploying this out as a model for defense is that it's quite easy to go too far and damage the company more than the damage from the actual information leaking out.

This balance between security and functionality is critically important. It is not possible to eliminate all risk from operating in a business situation, and a decision must be made at how much risk the company is willing to take on. Until this level is set in an organized way everything is left to be one off decisions that won’t be inline with the actual company goals.

What can we learn from this? Although blocking or monitoring software and security awareness are good methods of protection, they were not fool proof or consistent throughout the company. This means that even if 9 out of 10 employees are secure, one still causes a breach.

What we did not see used at all in our calls where defenses like:
“I have to talk to my manager” or similar scripts where an employee is encouraged to give the user an excuse and pass them off to a person of higher rank. That does not, many times, mean that person is more security minded, but that pass off and delay will make some attackers too nervous to continue.

Additionally, a common tactic used by social engineers is a false time constraint. This leads to a high-pressure situation where the employee is much more likely to make a mistake due to not being able to think through the problem. By having a brief pause to the call, it gives the employee a chance to catch their breath and analyze the situation without these false time constraints.

Updated Software: In the cases where we were able to obtain the versions of the software used we saw things like IE6, IE7, Adobe Acrobat 7 and 8, etc. Updated software can be a great defense.

It must be remembered that in many cases, the social engineering aspect of an attack is to enable a follow-up technical attack. By limiting the software in use and ensuring that it is up to date, the overall attack surface is decreased.

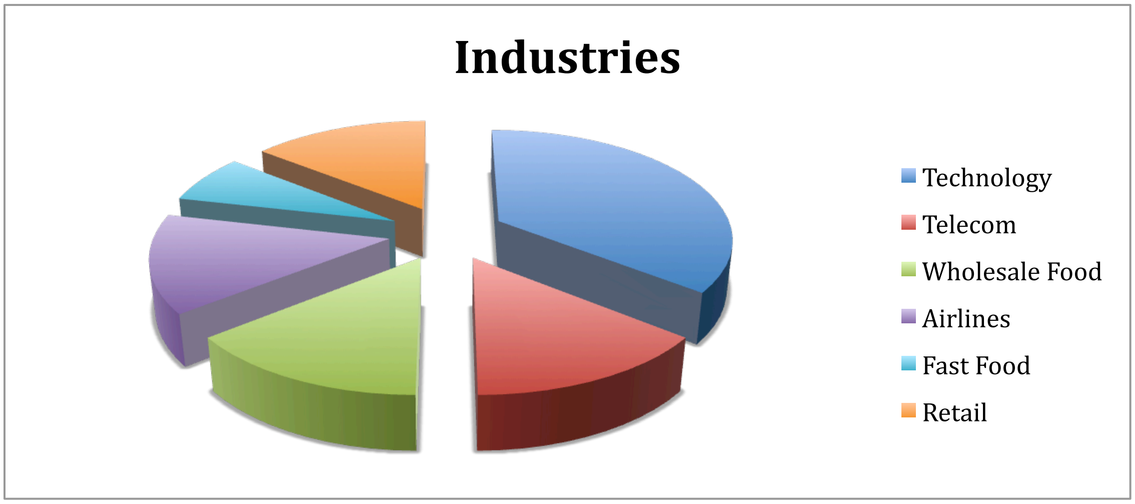
Higher quality awareness training. Out of the companies that had awareness training, only one seemed to be truly more difficult to infiltrate. Most attackers simply made another call and found a person willing to give the attacker all the information requested.

Having multiple targets gives the social engineer tremendous power. Completeness in your defense is critical.

Hang up. Out of the few reps that put up a fight, none simply just hung up, regardless of the pressure put on them by the social engineer to give up data.

Industries Targeted

This year we targeted a very specific subset of industries: technology, telecom, wholesale foods, airlines, retail, and fast food. We decided to mix up the types of industries to determine if the level of insecurity we saw at DefCon 18 would exist across the map of industries at this year's DefCon.

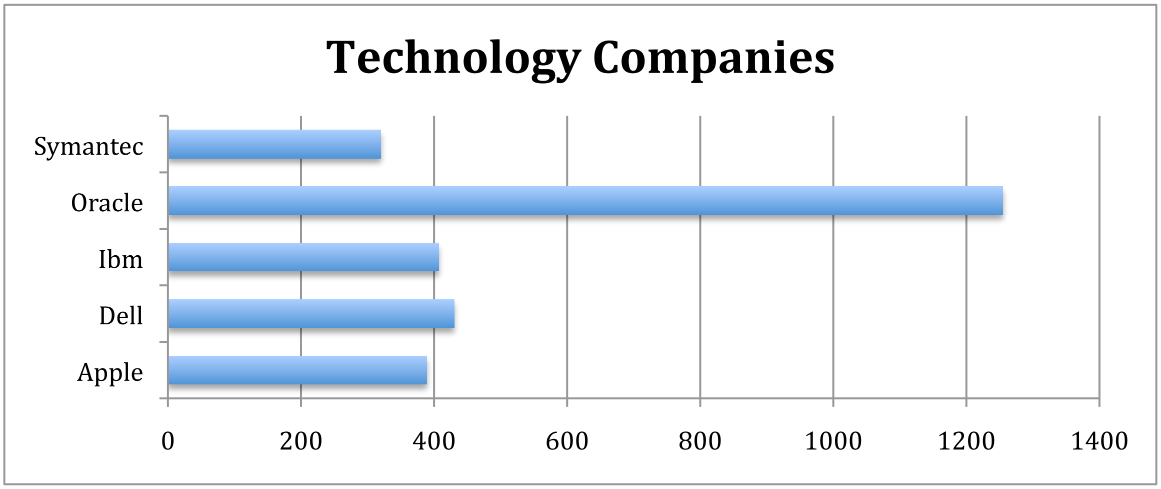


How did companies compare to each other inside the same industries? Below are charts showing how each company compared to a competitor in the same industry. The ratings are based on score minus the SEORG Index rating given above.

The higher the score, the lower the level of security. The goal is to be scored as low as possible as a higher score is an indicator of insecurity.

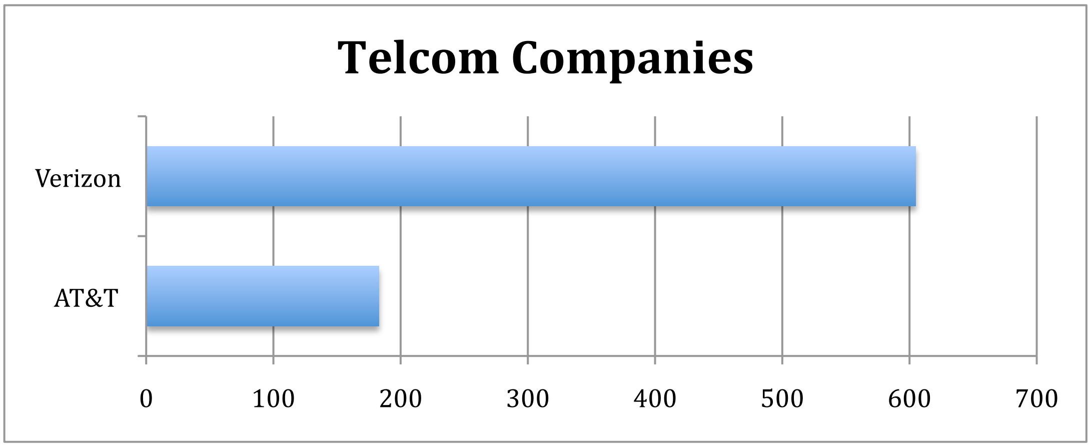
We want to stress that the success at obtaining information from a target depends largely on the person they reached and the skill of the caller.

Technology: Apple vs. Dell vs. IBM vs. Oracle vs. Symantec



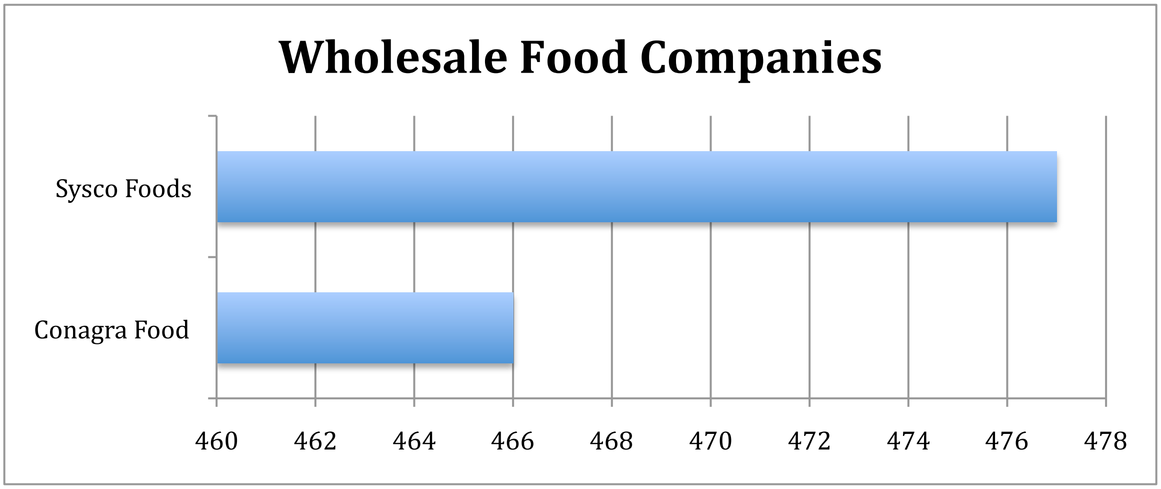
Overall, Symantec defined itself as one of the most secure companies.

Telecom: AT&T vs Verizon



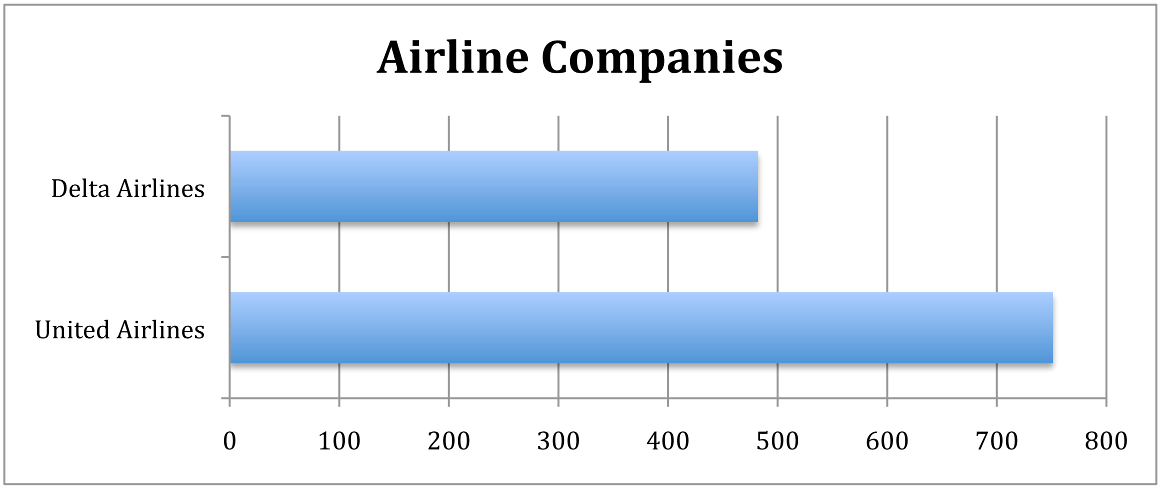
In the case of the two telecom giants, AT&T was very resistant to our attempts. AT&T openly defied the caller a few times and even rejected the advances in numerous settings. AT&T's retail stores were called, where as Verizon's customer support lines were called. The results were much different for the caller to Verizon as shown above.

Wholesale Foods: Conagra Foods vs Sysco Foods



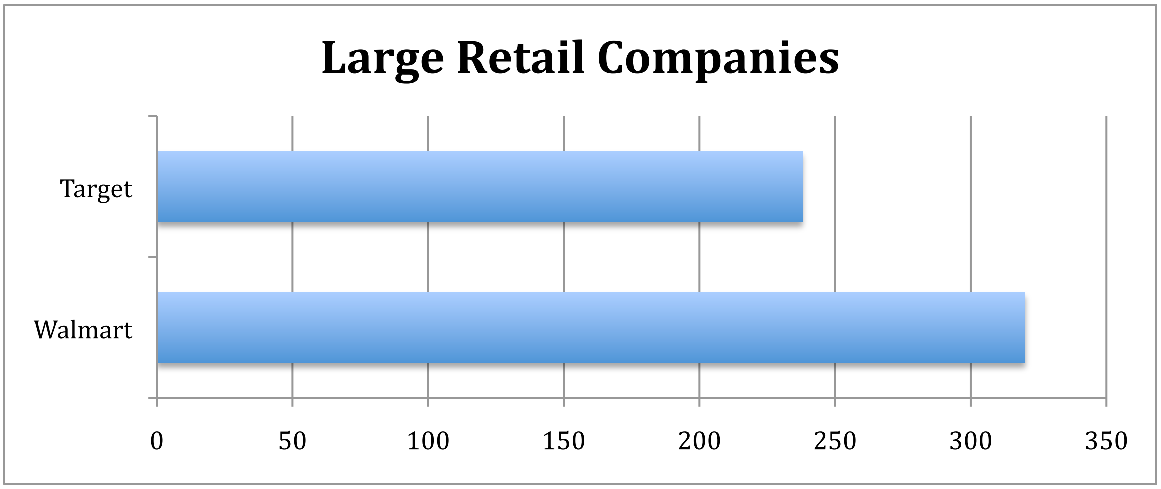
Even though the scores look much different in this one, it is a close match. Both scored in the mid 400's. Both companies need large-scale improvements to their security policies and awareness training for employees. They both scored quite high on the rating scale, indicating a higher degree of insecurity.

Airlines: Delta vs United



Although the scores look very different, the bulk of the scoring difference comes from the passive information gathering stage of the competition. That is not to say it is not dangerous; we just want to point out that the bulk of the insecurity is not due to the calls made or individuals called.

Large Retail: Walmart vs Target



Last year, retail proved to be a formidable foe for social engineers at the CTF. This year retail again showed it strengths. Retail shows that it withstood social engineering attempts more readily than any other counterpart. Even AT&T's great score can be attributed to the fact that their retail stores were called.

Corporate Security Spending

We do not have access to the budgets and internal documents of each target company, but through research we were able to obtain things like: number of employees, total revenue, level of spending on all IT, and the percentage, on average, spent on security.

Armed with this knowledge, we can come up with a general idea of what each industry and company has spent on security. This will include all security based spending whether it is security awareness, hardware, software, penetration testing, training, and all other avenues of corporate spending for security.

Below we have created a simple chart to show this corporate spending on IT Security.

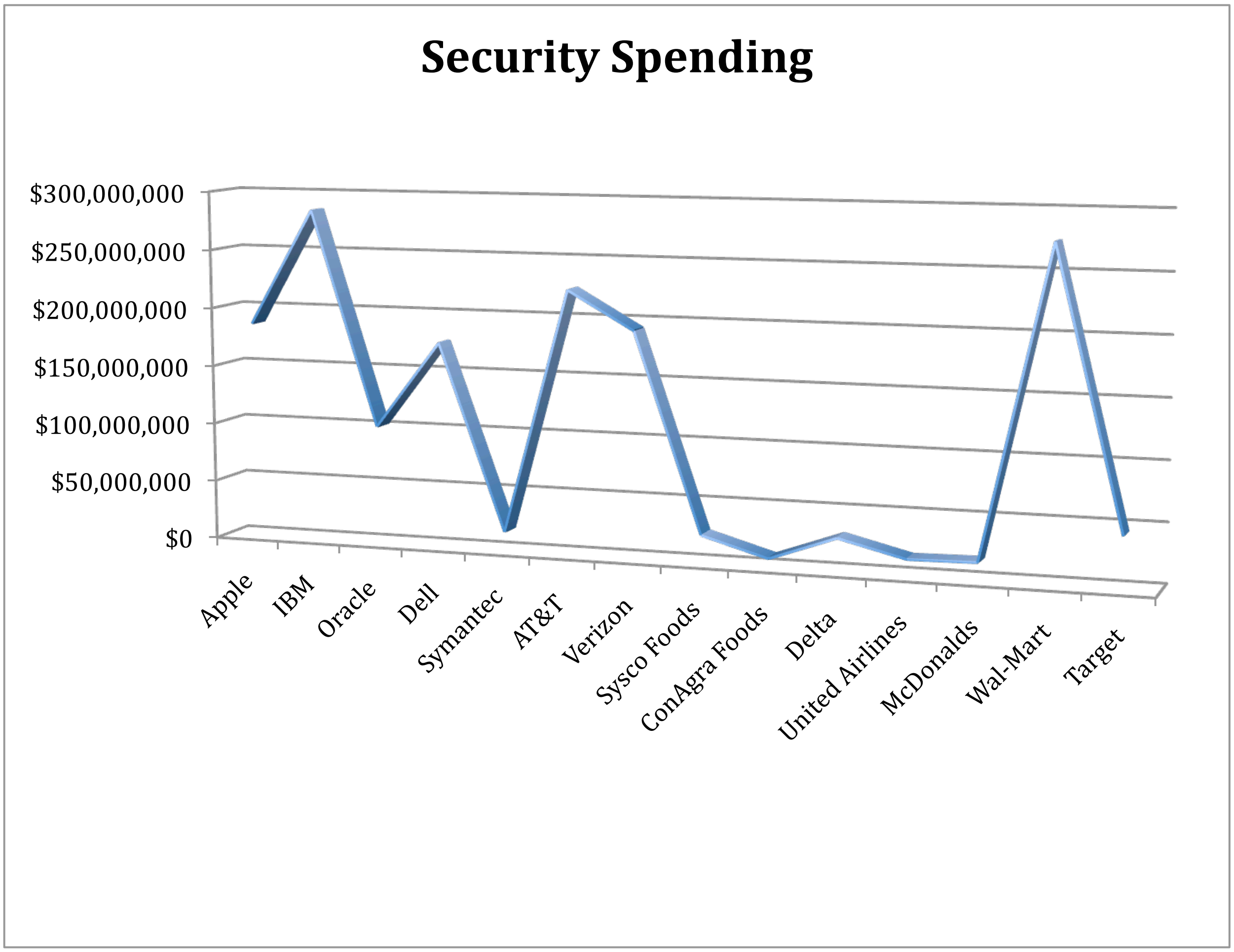
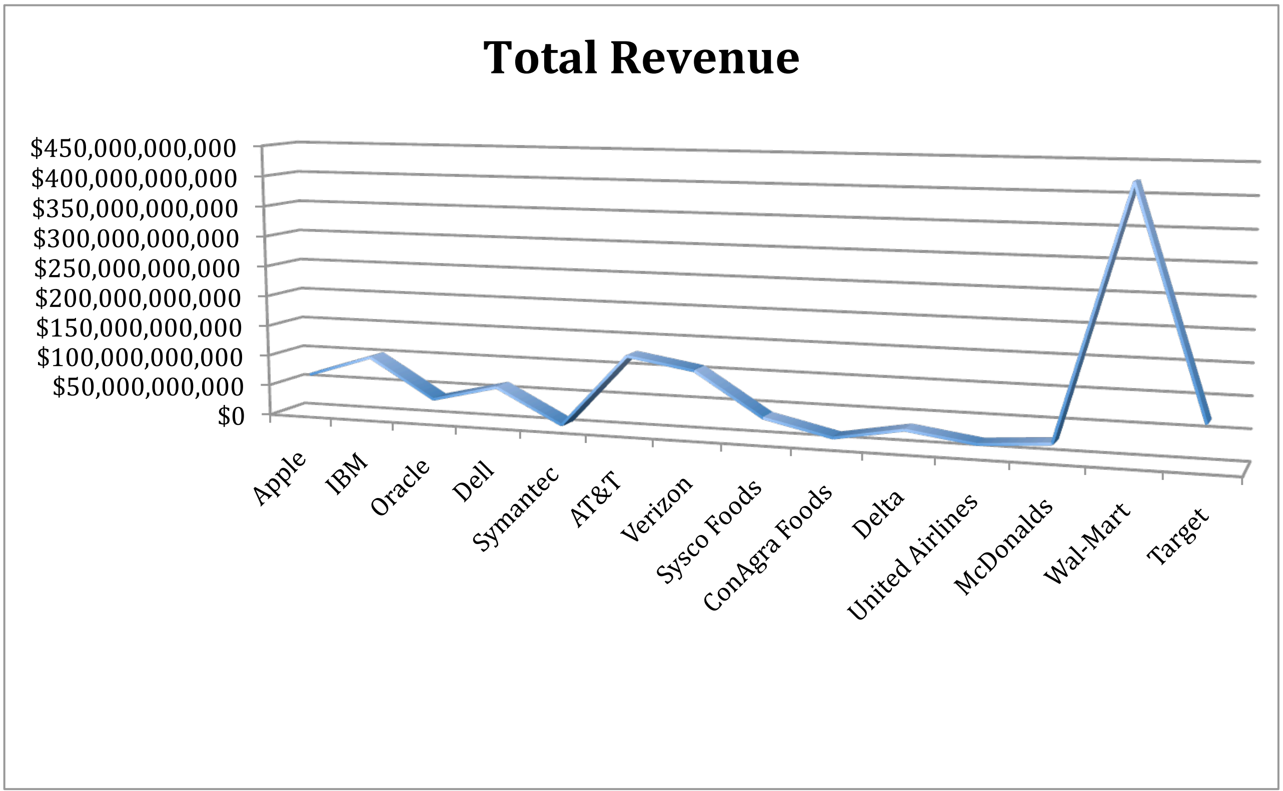


Figure 1: Based on statistics from Gartner*

- Figures based off of: Gartner IT Key Metrics Data (Dec 2010. Ione-de-Almeida-Tendencias-2011, http://www.darkreading.com/security/security-management/225701261/index.html and Hoovers.Com

How do these figures compare to their total revenue?



Is there a direct correlation between IT Security Spending and how each company fares against social engineering attempts?

We cannot, for fact, state that there is a direct link between security spending and how a company fared in this competition. What we can say is that it appears that companies who spent less did worse. AT&T, who was one of the leaders in this year's competition, also had one of the highest spending on corporate security. The second highest performing company was Target and their budget was half of AT&T's. Overall, IT Security spending (according to Gartner and Forrester) is about 5% for each company.

We believe there is a more direct relation to the style and frequency of security education than to amount spent. AT&T employees boasted of monthly security awareness training and the results showed this to be true.

Conclusion and Recommendations

Although there were some industries and some companies that proved to stand out from the rest, in the end, all of the companies would have received a failing mark in a real social engineering penetration test. While there are many conclusions that could be drawn from our results, the most important is: There is ample information floating out there that malicious social engineers can use to target the average company. This information can be put to use by the average, inexperienced social engineer to bear devastating results. This is consistent across all tested industries, with professional organizations appearing to be the most vulnerable.

What this means is the barrier of entry for social engineering attacks is very low. Criminal enterprise is like any other business; return on investment is important. The investment required for social engineering attacks is far lower than other attacks, making them the most likely approach. Due to lack of attention paid to this threat, there is no indication that this situation will change soon.

In light of this information you would expect to see companies, especially Fortune 500/1000 companies, regularly conducting social engineering penetration tests and risk assessments.

Sadly, that is not the case. Why?

Many companies have the mentality of, "It won't happen to us.", or "Our people won't fall for that." The sad truth is, those are the very people that will and do fall victim to these attacks, as demonstrated by the contest.

What can be done to correct the situation?

It would be impossible to list all the different things that could be done to rectify the security situations in these companies, but we wanted to name three things that could be done.

1: Social Media Policies

Companies should carefully plan out how they want to manage their employee's use of social media. Clear definitions of what is allowed and what is not allowed should be put in place. If hobbies, vacations, and other parts of personal life are being discussed on these sites, business should not be mixed in. Guidelines and policies can help the employees understand the risks associated with social media usage. In addition, clear defined policies on how, where, and what kind of documents can be uploaded to unsecured area of the Internet can go a long way to safeguarding companies.

2: Consistent, real world education

The lack of quality, consistent, and effective security awareness training was clearly seen through the results of this year's Social Engineering CTF. In the one company that had monthly training and awareness, the employees were much more aware of potential threats and dangers and therefore were more successful and stopping social engineering attacks.

Security awareness training needs to be consistent, frequent and personal. It doesn't mean that a company needs to plan large events each month, but annual or bi-annual security reminders should be sent out to keep the topic fresh in the employee's minds. There has been success at making it a "game" where employees compete to find, identify and notify the proper channels in regards to social engineering attempts on the company. Security education really cannot be from a canned, premade solution. Education needs to be specific to each company and in many cases even specific to each department within the company.

3: Regular Risk Assessment and Penetration Test

Still one of the most necessary aspects of security is the social engineering penetration test. When we perform social engineering risk assessments, we identify all areas where a company is vulnerable to attack. Leaked information, social media accounts, and other parts of the company are identified, cataloged and reported on. Potential vectors are presented and mitigations are discussed.

A social engineering penetration test takes things to the next level, where those vectors are not just written about but tried and executed. The results are used to develop awareness training and can truly enhance a company's ability to be prepared for these attacks.

These are just three of the many strategies that can be utilized to help 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. If you, or your organization, have questions regarding any aspect of this report please contact us at: defcon@social-engineer.org or at the contact information below.

About Social-Engineer.org & Social-Engineer.Com

Social-Engineer.org was developed to be the authority on the topic of social engineering.

Malicious parties have always been interested in obtaining real return on investment on attacks. With the advent of stronger and more universal protection systems in various networked systems, this has caused an increase in the cost required to successfully execute an attack against modern systems. This has caused many attackers to move to a lower cost avenue of attack, namely targeting people.

Social-Engineer.org has documented the manner in which these tests are conducted to increase awareness of this increasingly active attack vector. Only by understanding how these attacks are conducted can we build proper and effective defense.

Security through education.

Social-Engineer.com is the natural progression of all the work that has been produced from Social-Engineer.org. After creating the world's first web based social engineering framework, many companies came asking for assistance in social engineer penetration testing, risk assessments, and security awareness training.

We are preparing to launch the first ever Social Engineering for Penetration Testers course in March of 2012 and will continue to provide, support, and manage the free newsletter and podcast that so many companies use.

Sponsors

The Social-Engineer.org CTF event was made possible through the support of the following organizations:

Professional
Social Engineering
Services and Training
SOCIAL-ENGINEER.COM

QUALYS®
ON DEMAND SECURITY

Professional Training and Tools for Security Specialists.
OFFENSIVE
security

CORE®
SECURITY TECHNOLOGIES

EFF
ELECTRONIC FRONTIER FOUNDATION