tracesecurity
Compliance, simplified.

White Paper

Call Centers: A Gateway for Social Engineers to Access Your Company's Most Sensitive Information

While companies commit huge budgets and resources on complex technology to fortify their network perimeters, their own employees may be giving dangerous cybercriminals the keys to the front door.

Overview

In its most basic form, social engineering is the act of manipulating someone into doing something they normally would not do. For our purposes, we will consider social engineering the art form of using deception and manipulation to persuade an unsuspecting person to perform actions like divulging confidential information or allowing unauthorized access to sensitive data.

The area most susceptible to a successful breach isn't a company's network perimeter or web applications…it is actually customer support. The relatively weak controls applied to a customer support center expose the company's most important assets reputation, corporate information, and customer data – to extremely high levels of risk.

This paper explores the rationale as to why customer support centers – most notably the call center – is such an attractive target to social engineers. We will not only analyze the fundamental causes for most security weaknesses within call center environments, but also provide reliable strategies for mitigating risk and reducing exposure. Plus, we shall expose the common methods of attack used by cybercriminals, explain why they work, and offer expert insight on what organizations can do to identify and combat malicious social engineering tactics.

Why Social Engineers Target Customer Support Centers

It may sound counter-intuitive that a company's customer support centers are the preferred target for social engineers seeking to steal information and data. However, when you consider that this class of criminals selects targets of opportunity that can be exploited with minimal effort, offer a low risk of being discovered, and have the potential for a high payoff, it quickly becomes apparent why customer service environments – like call centers – are regarded as such a high-priority mark.

TraceSecurity has performed hundreds of social engineering engagements across a wide range of industries, including comprehensive testing of internal and outsourced call centers at major corporations. Through our extensive experience, we have identified four major reasons why social engineers consider call centers to be attractive targets.

#1: A "One Stop Shop" of Valuable Data

Customer support employees have the ability to give a social engineer access to almost all the information he considers valuable; ranging from fairly innocuous, to highly sensitive. This makes call centers a "one-stop-shop" for cybercriminals looking to steal valuable information. Information that tops their shopping lists includes the following:

1. Profile information from accounts such as a passwords or gamer data, which allows the criminal to tap into free services or build an elaborate "pre-text" that may be used to further escalate a larger breach
2. Confidential personal data such as credit card information and social security numbers that can be leveraged for identity theft
3. Bulk account information that can be exfiltrated during a single engagement and lead to a large scale breach

#2: The Human Factor is Far Easier to Compromise Than Technology

When the types of technological controls used to protect a network infrastructure are compared against the relatively subjective countermeasures present in a call center environment, it becomes clear that the human factor presents extremely exploitable weaknesses.

Network infrastructures rely on layers of advanced technological controls that are built on emotionless "black and white" decision engines that cannot be persuaded to ignore their preprogrammed parameters. In contrast, companies generally rely on the employee as the primary security control within a call center environment. But the main goal of a customer service employee is to help solve problems and provide exceptional service. Besides, unlike technological safeguards, humans are influenced by their emotions during the decision process. A social engineer can take advantage of these emotions through persuasion, pressure, guilt and others to cause the employee to break protocol.

Remember, your customer service representatives are constantly weighing the need for security with the need for good customer service; sometimes, these two factors are difficult to balance. It only takes simple lapse in judgment to expose your sensitive data.

#3: Impersonation is Easy When So Much Information is Available

Compromising a call center is a relatively low-tech attack method that is predicated on the social engineer's ability to establish credibility and trust with an employee of the targeted company. To accomplish this, he must devise a believable story – or a "pre-text" - based on as much factual information as possible. Some of the most successful pre-texts are based on legitimate information about a customer, a fellow employee or even a member of upper management.

Ironically, the potential victims of a cybercriminal inadvertently help streamline his job! Given that most companies post volumes of information about the organization, its employees and its practices through-out various online sources, forming a pre-text is a fairly easy task. The problem is further compounded because the company's employees, as well as their customers, readily share personal details like contact information, birthdays, and even work-related data throughout various social networks. Thus, it becomes exceedingly simple to collect legitimate information that helps enhance the pre-text and makes it easier to convince a call center employee they are who they claim to be.

#4: The Chance of Discovery is Low

Establishing credibility and trust within the first few moments greatly reduces the chance a social engineer will easily be discovered. As discussed above, most criminals will spend the time and effort to create a credible pre-text based on just enough verifiable information so that the elaborate lie can withstand at least a minimal amount of scrutiny, thus making it easier for the criminal to convince the unsuspecting employee they are a legitimate caller.

Seasoned social engineers further sell their believability by employing additional tactics prior to the call, such as spoofing their caller ID to match that of a customer or another department within the targeted company, or sending the call center employees a convincing spoofed email from a trustworthy source, like upper management or the IT department. When used in unison, these tactics make it extremely difficult for employees to distinguish between a fraudulent caller and a genuine caller.

Sadly, social engineers almost never get caught during the actual attack. Even when their cover is blown by a skeptical customer service representative, the criminal faces virtually no consequences other than having to create a new pre-text. Tracking down a would-be social engineer is incredibly difficult and rarely successful. Unfortunately, social engineers tend to get caught only once the breach has occurred and the criminal is attempting to use or sell the stolen information.

Based on hundreds of engagements, TraceSecurity has found that the above four factors seem to be universal constants - regardless of the size of the company or type of industry. In fact, when TraceSecurity analysts are preparing for social engineering engagements, these factors are taken into consideration when choosing an attack pathway and methodology. Professional social engineers also recognize that these characteristics apply to virtually every call center environment so there is no motivation for them to stop targeting call center employees.

The Call Center Employee vs. the Social Engineer

Pitting the call center employee against a social engineer is an unfair fight. Not only are these con artists experts at persuasion and manipulation, but they are also willing to use any type of deception to get what they want. The typical customer support employee is trained to be accommodating and helpful. So, if you contrast the deceptive nature of social engineers with the passive "people pleasing" attitude of the typical call center representative, it is obvious that the criminal will most certainly have an ethical (or in this case, an unethical) advantage.

It is ironic that these essential traits for a customer service employee are actually a handicap in the fight against fraud. Criminals recognize the ingrained doctrine of 'the customer is always right' as a security weakness and leverage the employee's fear of customer complaints, or even the perception that they provided poor service, as an effective tool of persuasion.

According to Chris Hadnagy, the lead developer and founder of Social-Engineering.com and organizer of Defcon 19's Social Engineering "Capture the Flag" contest, a recent real-world exercise that exposed significant security weaknesses at some of the biggest corporations' call centers, views the people-pleasing nature as an inescapable truth. "The nature of these customer service jobs is to develop a mindset that 'the customer is always right'. And while this is an essential attitude for providing good service, the side-effect is that the representatives are constantly in the mode of answering questions and providing information…which tends to make a social engineer's job much easier."

The results of social engineering engagements conducted by TraceSecurity consistently show that customer service agents are more than willing to provide crucial account information...even without being pressured to do so! TraceSecurity's tests reveal that the most common failure points involve "pulling on the hearts strings" of customer service agents by employing common pre-texts of the caller being deployed overseas, a parent in a desperate situation with a child or a coworker needing access to a terminated employee's files. These popular approaches appeal to the agent's empathetic response and lead to failure because of their desire to simply provide good customer service. Through these tests, we have found that employees readily offer all sorts of sensitive data without being prompted, ranging from seemingly innocuous account information - like the type of account - to critical information like providing hints to the answers of secret questions necessary for authentication.

Results From A Real-world Scenario

In one case, TraceSecurity testers made 200 social engineering calls to the customer service center of a large, multinational organization in an attempt to manipulate the call center agent into providing additional account information. Our testers were given only minimal data from established "seed accounts" (information from seemingly legitimate accounts), and employed common pre-texts, such as restoring access/changing information in the wake of a natural disaster, after a divorce or the death of a spouse, after a spouse has been deployed overseas, or when a parent trying to limit their child's access.

This particular test resulted in:

- Over 25% of calls led to a Total Compromise, where enough information was divulged so that the account could be accessed by the tester
- Over 40% of calls were Partially Compromised, where enough data was provided so that the tester could leverage it during a future call to possibly achieve a Total Compromise
- In no instance was the TraceSecurity tester "caught in the act" or even identified as a threat

These results clearly indicate that if a caller has just enough basic information, combined with a believable and relatable sob story, most employees will exhibit empathy by ignoring policy and procedure in order to help the caller solve a problem – or at least help them along – during their time of need.

As demonstrated by the results of the above test, social engineers won't strike gold with every swing. But the results also indicate that they never get caught in the act; therefore, when a real-world criminal fails to elicit sensitive information from one call center employee, he simply calls back until he connects with a different employee and begins the process again. It seems that social engineers truly believe the old cliché, "if at first you don't succeed...try, try again."

The 2011 Social Engineering Capture the Flag Contest, "The Schmooze Strikes Back"

A group of contestants participating in a social engineering "Capture the Flag" event at the 2011 DefCon conference in Las Vegas demonstrated how easily even the most sophisticated customer contact centers could be tricked into divulging potentially harmful information.

The 14 companies chosen were no "easy marks". The targets included some of the biggest, most well-known companies such as Apple, AT&T, Conagra Foods, Dell, Delta Airlines, IBM, McDonalds, Oracle, Symantec, Sysco Foods, Target, United Airlines, Verizon, and Walmart.

The goal for contestants was to ferret out specific information, or "flags", during either the information gathering stage or the actual engagement. Each flag represented non-sensitive data about the inner workings of the target company. The contestants, ranging from skilled social engineers to unskilled enthusiasts, were allowed 2 weeks prior to the event to research and compile information on their assigned targets. It is important to note that the contestants only used passive information gathering techniques to establish their pre- texts; direct contact with the target was strictly prohibited.

Contestants used this information to develop realistic and believable pre-texts in order to pose as customers, fellow employees, or even members of upper management. During the actual contest, the participants were given 25 minutes to contact their assigned target, conduct the social engineering engagement, and collect as many high value flags as possible.

The results were startling: all 14 targets divulged potentially harmful information to the contestants, and only three employees offered any type of resistance to the social engineering techniques.

Even more alarming was that contestants were able to persuade employees from every targeted company to visit a "dodgy" URL!

"Our goal was to demonstrate the security weaknesses at call centers...not to create a full-blown breach." said the event's organizer, Chris Hadnagy. "But it is conceivable that a malicious criminal could do the same thing we did, only with much more devastating results."

Hadnagy, who is also the lead developer of the Professional Social Engineering Team at Social-Engineer. com, points to the fact that employees from each company were willing to visit the URL when requested by the contestant. "That clearly indicates a lack of basic security awareness training as well as inadequate organizational policies & procedures."

In a real-world scenario, the URL could have been seeded with a variety of malware that, when visited, could have infected the employee's workstation and wormed its way into the central network.

The Costs of a Data Breach

In their 2010 Annual Study, U.S. Cost of a Data Breach, Ponemon concluded that data breach costs have steadily risen over the past 5 years, topping out in 2010 at an average cost of $7.2 million, up 7 percent 2009. Ponemon's results show data breaches cost their companies an average of $214 per compromised record, up $10 (5 percent) from the previous year.

The most expensive breach denoted in the study cost one organization $35.3 million to resolve the loss of 105,000 records. The least expensive breach cost a company a whopping $708,000 to rectify the loss of only 4,200 records.

According to Ponemon's metrics, the amount a data breach could cost a company depends on several factors, such as the industry it serves, the total number of records compromised, the length of time between detection and notification, and even the reason the breach occurred. For example, the cost to resolve a breach caused by malicious activity is an average of $318 per record...significantly more than one caused by a system failure, on average $210 per record.* Ponemon also reported that for the first time in the annual study's 6 year history, malicious or criminal attacks were the most expensive cause of a data breach...and not the least common one.

The primary cost centers related to a data breach include lost business due to churn, legal services, investigations and forensics, audit and consulting services, customer acquisitions, contact costs, compliance services, ID protection services, free or discounted services, and public relations.

Directs costs often include such expenses as outsourced customer hotlines, free credit monitoring subscriptions, discounts for future products and services, plus engaging forensic expertise.

Indirect costs include elements such as in-house investigations and communication and the extrapolated value of customer/ stockholder loss resulting from turnover or diminished acquisition rates, which is measured by customer turnover, or churn rates.

According to the report, customer turnover in direct response to breaches remains the main driver of data breach costs, topping out at $134 in 2010.

A metric that is exceedingly difficult to quantify, especially over an extended period of time, are the direct and indirect costs related to a badly damaged brand or company image. The expenses associated with recovering from months, or even years, of bad press are virtually incalculable. If well established companies find it extremely difficult to keep existing customers and attract new customers after a high profile security breach, imagine how daunting the challenges a small-to-mid-sized company must face in a post-breach recovery phase.

The Likelihood of a Social Engineering Attack

Having established that customer service centers are certainly an attractive target for social engineers, the next logical question is 'what is the likelihood of attack?' Based on the empirical evidence collected by various studies over the past 8 years, there has been an increasing trend of social engineering attempts on operations centers such as customer service departments and call centers.

According to Symantec's 2011 State of Security Survey, 20% of their respondents reported that their organization suffered social engineering attacks in the past year. Moreover, the respondents indicated social engineering attacks as the second fastest growing security threat, just behind malicious code attacks.

Ponemon's 2010 Annual Study, U.S. Cost of a Data Breach found that almost one third of all cases in the 2010 study involved a malicious or criminal attack. This figure is up 7 points from 2009 after having doubled in 2008. According to the study, 2010 was the first time malicious attacks were not the least common cause for breaches.

But the most compelling evidence comes from the recently released 2012 Verizon Data Breach Investigations Report. For the first time since it began publishing data breach information, the 2012 Verizon report began including statistics specifically on breaches resulting from social engineering attacks on call centers. The report reveals 3 significant data points:

1. **11%** of breaches caused by social engineering were directed at Customer Support staff (8% Call Center, 3% Help Desk)
2. **46%** of all the breaches caused by social engineering involved the use of the telephone, making the phone the #1 medium for social attacks
3. Social engineering tactics were used in **7%** of the total breaches, but accounted for **37%** of the records stolen during incidents that employed social tactics; pre-texting, phishing and elicitation (the subtle extraction of information in a conversation) accounted for over two-thirds of the methods used in those breaches.

This may seem like a lot of statistical data to digest, but the end result is that we now have analytics that support what most security industry experts have known for years. Social engineers use a combination of threat actions like pre-texts, phishing/vishing, and phone calls to extract information from unsuspecting call center and customer support staff. The report also makes the case that as companies shore up weaknesses in perimeter security, cybercriminals will naturally gravitate towards targeting the more vulnerable systems controlled by human efforts.

Documents referenced in this resource

Symantec's 2011 State of Security Survey: In its 2011 State of Security Survey, Symantec sought to update its global perspective on key security threats, trends and responses across a range of businesses worldwide, including SMBs and larger enterprises—3,300 in all. http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf

Ponemon's 2010 Annual Study, U.S. Cost of a Data Breach: the sixth annual study concerning the cost of data breach incidents for U.S.-based companies, sponsored by Symantec. http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_re port.pdf?om_ext_cid=biz_soc-med_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

2012 Verizon Data Breach Investigations Report: This comprehensive report analyzes 855 global data breach incidents and over 174 million compromised records in 2011to identify security trends. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Mitigating the Risks

Limiting their exposure to social engineering threats should be a top priority for any company; but it should be one of the highest priorities for organizations with internal customer contact centers as well as those who outsource those functions. Not only do the 3 leading data breach studies warn that it is only a matter of time before an organization experiences a serious social engineering attack, but the recent "Capture the Flag" social engineering exercise at Defcon 19 proves even the most sophisticated companies are exposed to enormous risks.

The first step in risk mitigation is to identify the level of exposure. For a call center environment, this can only be done by (1) ensuring the risk assessment accurately reflects the potential threats, (2) evaluating the effectiveness of policies and procedures regarding security, (3) training staff on the proper way to follow policy and procedures, and (4) testing risk factors that involve compromising the human element.

Risk Assessments

An organization's risk assessment must encompass the ever-present threats associated with social engineering and should accurately reflect the controls that are in place to mitigate the risks. These controls would typically be security awareness training and organizational policies and procedures.

However, management should be wary of over-emphasizing the effectiveness of these security controls because they are really only effective whenever the employee actually uses them. In other words, the level of protection offered by security training and policies is dependent on the employee's willingness (or ability) to follow the procedures established by the company.

This should be taken into consideration the next time an organization updates their risk assessment. Assigning a higher risk rating to the call center environment may indicate a compelling need for further testing or, at very least, enhanced security awareness training.

Information Security Policies

It is management's responsibility to ensure organizational policies clearly and accurately outline the processes and procedures necessary to verify information, establish a regiment of security awareness training, and also provide a framework for testing employees' understanding and adherence to the policies. It is imperative that policies do not contain ambiguous language or unclear protocols that leave room for interpretation because this could lead to an employee being able to justify divulging information they consider to be harmless or "non-essential".

Security policies should include provisions that empower employees, especially call center and customer support staff, to reject inappropriate requests or automatically escalate questionable requests to a supervisor without the fear of punishment. These simple actions will increase the chance that social engineering tactics, like phishing messages, spoofed emails or "bullying" techniques, will be properly identified.

Companies should also make sure the policies address evolving security issues. For example, social media policies should clearly define what employees are allowed to post and what information is prohibited from sharing on social media sites. In addition, the policy should state what types of company documents, if any, can be shared on an unsecured area of the website. This type of written guidance, along with frequent security awareness training, will help employees better understand their role in preventing data breaches and ultimately create a more secure workplace environment.

CompTIA's 9th Annual Information Security Trends Study found that 53% of IT and business executives say human error is more of a factor in security breakdowns today than it was two years ago. Two of the most common human errors that contribute to security breaches are the failure of end users to comply with security policies and lack of security training.

The fact remains that many organizations' policies and procedures are more than adequate to address the risks and threats related to social engineering. The issue may be that employees simply are not following correct processes, even though they are well aware of the established policies and procedures. Companies can address these types of scenarios by adding controls via policy that focus on employee accountability, as well as other types of procedural checks & balances.

Security Awareness Training

Social Engineering testing allows a company to assess its Information Security policies as well as the employees' adherence to those policies. Social engineering tests do much more than simply identify failure points and weaknesses; the results can help provide a framework for improving the organization's security awareness and training programs.

These tests involve experts posing as a "trusted authority" (such as a customer, employee, or partner) in an attempt to manipulate employees into divulging confidential information, allowing unauthorized access to systems, or compromising any other sensitive information. Testers use a variety of "real-world" techniques, including spoofed emails, phishing, vishing, and pre-texts, in order to thoroughly evaluate the company's risk exposure to potential social engineering threats.

Social engineering tests will demonstrate which specific tactics are successful within a particular organization. Because many of the techniques involved in these tests are designed to assess the human sympathy/empathy risk factors of the company's employees, the tests may identify the lack of a specific policy or employees' failure to understand the policies.

At a more granular level, concentrated failures within a particular group of employees, such as entry-level positions, would suggest that more education for that group should be mandated. A common scenario is when companies see that new employees consistently fail the tests, they automatically enhance their initial training for new hires. Less common is evaluating if the company's more seasoned staff are experiencing high failure rates. A good social engineering test should reveal these trends and help identify detailed mitigation strategies, like more frequent "real world" training to boost the awareness at each level of the staff.

Employee training that is based on the results of a genuine social engineering exercise will strike a chord with staff members because, after all, the incidents actually occurred in their department or company! The training should address any identified weaknesses and provide instruction on how to handle situations they are most likely to experience in their day-to-day interactions. These types of relevant exercises reveal the potential exposure that could be caused by an unethical social engineer without the risk of compromising real data.

Social Engineering Tests

Social Engineering testing allows a company to assess its Information Security policies as well as the employees' adherence to those policies. Social engineering tests do much more than simply identify failure points and weaknesses; the results can help provide a framework for improving the organization's security awareness and training programs.

These tests involve experts posing as a "trusted authority" (such as a customer, employee, or partner) in an attempt to manipulate employees into divulging confidential information, allowing unauthorized access to systems, or compromising any other sensitive information. Testers use a variety of "real-world" techniques, including spoofed emails, phishing, vishing, and pre-texts, in order to thoroughly evaluate the company's risk exposure to potential social engineering threats.

Social engineering tests will demonstrate which specific tactics are successful within a particular organization. Because many of the techniques involved in these tests are designed to assess the human sympathy/empathy risk factors of the company's employees, the tests may identify the lack of a specific policy or employees' failure to understand the policies.

At a more granular level, concentrated failures within a particular group of employees, such as entry-level positions, would suggest that more education for that group should be mandated. A common scenario is when companies see that new employees consistently fail the tests, they automatically enhance their initial training for new hires. Less common is evaluating if the company's more seasoned staff are experiencing high failure rates. A good social engineering test should reveal these trends and help identify detailed mitigation strategies, like more frequent "real world" training to boost the awareness at each level of the staff.

Employee training that is based on the results of a genuine social engineering exercise will strike a chord with staff members because, after all, the incidents actually occurred in their department or company! The training should address any identified weaknesses and provide instruction on how to handle situations they are most likely to experience in their day-to-day interactions. These types of relevant exercises reveal the potential exposure that could be caused by an unethical social engineer without the risk of compromising real data.

Repetition is Key to Success

The combination of an ever-changing threat landscape, the consistent evolution of malicious tactics, a typically high turnover rate of customer support staff, and the natural tendency for employees to let their guard down all contribute to keeping a company's security awareness posture in a constant state of fluctuation. This necessitates that organizations establish repeatable processes in order to effectively control the ongoing risks.

The cornerstone of an organization's security awareness program is performing and updating their information security risk assessment on a regular basis. This critical function will allow the company to maintain an up-to-date view of their risk exposure, as well as an accurate evaluation of the potential impact certain threats could have on their security posture. IT Risk assessments can also provide a framework for developing – or refining – security awareness training.

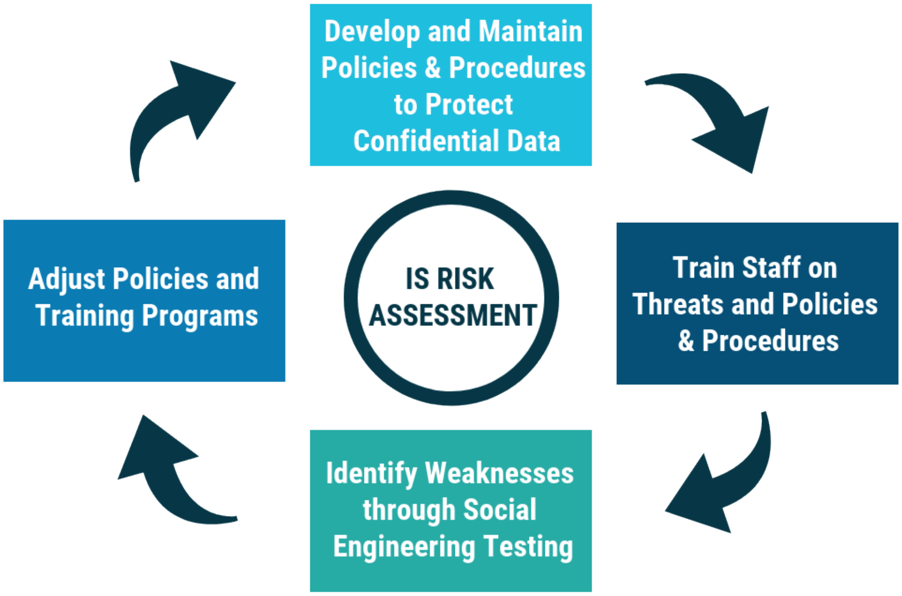
To be effective, security awareness training must be both consistent and frequent. TraceSecurity has found that it is much better to have a series of short, focused training courses over the course of a year rather than one exhaustive annual session. A primary driver for multiple training sessions each year is the fact that social engineering tactics are in a constant state of evolution. Criminals know that what worked yesterday may not work today, so they are continually modifying and adapt their tactics in order to bypass existing countermeasures and improve their success rates.

> “TraceSecurity’s social engineering tests brought a higher level of awareness to the organization which allowed us to make internal changes based on the results of those tests.”
>
> - Kelley Ferguson Director of Network & Security at Numerica Credit Union

Therefore, it is imperative that organizations periodically perform formal social engineering tests to evaluate how their policies, procedures, and training hold up against the current threat landscape. Periodic testing will identify consistent failure points, and allow the company to allocate sufficient resources toward shoring up those weak areas.

Organizations that choose to outsource call center functions should beware of the false sense of security that may arise as a result of that type of partnership. TraceSecurity has found that our customers who outsource their call centers face equal, and sometimes even greater risk levels compared to internally managed customer support centers.

We recommend companies do not rely solely on the tests and assessments performed by their outsourced call center partner, because, quite frankly, a 3rd party call center provider simply does not have as much at stake. Even if the provider hires excellent social engineering firms to conduct the various tests, the scope of those tests may not be adequate to identify all the vulnerabilities and weaknesses that could impact the organization. In these cases, management should consider performing independent assessments to ensure the employees of the call center are adhering to the organization’s policies and procedures. After all, history has shown that the media only focuses on the organization’s name after a breach...the 3rd party call center provider is usually just a footnote.


Develop and Maintain Policies & Procedures to Protect Confidential Data
Train Staff on Threats and Policies & Procedures
Identify Weaknesses through Social Engineering Testing
Adjust Policies and Training Programs
IS RISK ASSESSMENT

> “TraceSecurity’s social engineering tests were a valuable experience and allowed us to revolutionize our security procedures.”
>
> - Jason Berridge President and CEO Complex Community Credit Union

Summary

Social engineers seek out targets of opportunity that offer a low risk of being discovered, present easily exploited weaknesses, and have the potential for a high payoff. Most customer service departments meet these criteria because (1) the employees have unfettered access to a wide range of sensitive information; (2) are predisposed to being agreeable, usually lack adequate training, & can be manipulated much easier than technology; and (3) there is very little chance of being caught.

The leading industry studies indicate that social engineers have long recognized the weaknesses in call center environments, concluding that social engineering attacks have increased in each of the last few years, and almost a third of data breaches involve social engineering tactics. The elements of a business most at risk from a data breach are the company's revenue streams, its future productivity, it's organizational, customer, or employee data, and damage to a company's reputation and brand. While the average cost of a data breach is at an all time high of $214 per record, the costs increases even more to an average of $318 per record when the breach is a result of malicious activity. In addition, it is exceedingly difficult to calculate the long-term financial impact to a company after it experiences a breach.

The first step in combating the threats associated with social engineering is to conduct a comprehensive risk assessment that encompasses the threats posed to the customer service center. The results of the risk assessment will reveal the threat vectors that have the highest level of risk, determine the likelihood that a potential vulnerability may be exploited, establish the potential impact each threat would have, and identify the appropriate controls for mitigating risk within each vector.

Policies are crucial to establishing the overall framework of the company's information security program. Not only should these documents delineate the processes and procedures employees must follow, they should also outline how frequently training is conducted and the protocol for testing employees' under-standing and adherence to the organization's policies. Management may consider including provisions that help employees better understand their role in maintaining a secure workplace.

Frequent and focused security awareness training is a critical component of information security. Training should be tailored to the specific needs of each department and reflect the "real world" scenarios the employees are most likely to experience. The costs of providing quality, effective training is only a fraction of the costs incurred from even a relatively small security breach.

However, only by conducting thorough social engineering tests will an organization be able to assess how effective the existing security controls are in protecting the organization or accurately identify failure points or weaknesses. Companies that outsource call center functions should perform independent tests to ensure the employees of the outsourced provider adhere to the appropriate policies and procedures. The results of these types of tests can be leveraged to improve the company's security posture, such as developing additional training that addresses specific failure points or reevaluating ineffective policies and procedures.

A company's best protection against social engineering is to have (1) an understanding of its risk posture, (2) comprehensive policies and procedures that address the ever-changing threat landscape of social engineering, (3) a well trained frontline staff that is able to recognize and react to social engineering tactics,(4) periodic social engineering testing that verifies the effectiveness of policies, training and other controls, and (5) a commitment to consistently repeat the process and adjust the program as needed. The combination of these attributes give a company the peace of mind of knowing that weaknesses are constantly identified and addressed, as well as verifying that their security awareness training is working.

About TraceSecurity's Social Engineering Solutions

TraceSecurity is considered the top authority in Social Engineering testing. Our expert analysts have conducted hundreds of social engineering engagements, including performing tests of both internal and outsourced call centers, for companies across a wide range of industries. We also provide a comprehensive cloud-based solution to address all the necessary functions associated with security training and policy management.

Overview of Our Solution

TraceSecurity's social engineering tests not only identify weaknesses that may exist within a call center environment, but are also designed to evaluate several critical areas of information security. These areas include how effective the organization's policies and procedures are in mitigating social engineering threats, how well the employees adhere to the established policies and procedures, and the level of security awareness that exists among employees.

Before the actual engagement begins, TraceSecurity's analysts will coordinate with the organization to scope out the testing parameters. The scope of work establishes a framework for the engagement and determines how the testers will proceed, what kind of data (if any) will be provided to the tester before-hand, what types of scenarios will be used for developing pre-texts, and the point at which an individual engagement will be considered a "compromise" (i.e.; if a certain number of data points are divulged, or if a specific piece of data, like an account number, is revealed).

When conducting these tests, TraceSecurity experts pose as legitimate customers in order to manipulate an organization's employees into divulging as much confidential information as possible. The techniques used during the engagement are customized based on the goals of the organization. For example, the tactics deployed to compromise individual accounts (like posing as a customer) are different than those used to escalate network privileges in order to access extremely sensitive data, as in a scenario where a tester poses as a fellow employee or member of management.

After the initial engagement, TraceSecurity provides the organization with detailed logs of each call, email or form entry, which often not only reveals the security baseline within the company's call center environment, but also identifies consistent anomalies that may significantly impact the overall security posture. TraceSecurity also finds that most customers use the results to refine their priorities for future social engineering tests because they can now hone in directly on the most important weaknesses. From there, the test results are compiled into a comprehensive report that can be leveraged to create a frame-work for remediation efforts as well as a customized training program.

Solutions to Address Ongoing Training

It is clear that a well trained, responsive staff can greatly mitigate the risks posed by social engineering tactics. What is not always clear is how to go about creating and maintaining an effective information security training program.

In addition to offering onsite security training conducted by some of the most experienced security professionals in the industry, TraceSecurity provides a unique cloud-based solution for developing and managing a customized security training program. Organizations can leverage the TraceTrain module within TraceSecurity's ComplianceManager platform to customize online educational courses for multiple groups, administer tests to staff, and have the results automatically logged and tracked. As an added benefit, organizations can even use TraceTrain to develop and deploy customized web-based security awareness courses to their customers or other end users via their own websites! This valuable feature not only helps reinforce your company's commitment to maintaining a strong security posture, but also helps satisfy current and pending customer awareness education compliance regulations.

Our Industry-Leading Experience

Leading the charge in combating social engineering threats is Jim Stickley, TraceSecurity's CTO and cofounder. Jim has been involved in thousands of security services for financial institutions, Fortune 100 corporations, healthcare facilities, legal firms, and insurance companies. Through the years, Stickley has discovered numerous security vulnerabilities in products such as firewalls, PKI servers, online banking applications, and PDA devices.

Jim has been a consultant for the network stations FOXNEWS, CBS, NBC, as well as the Associated Press. Stickley has been featured in numerous magazines and newspapers, including Time Magazine, Business Week, Fortune Magazine, New York Times, PC Magazine, CSO Magazine, and hundreds of other publications. Stickley has also been showcased on numerous television shows including NBC's "Nightly News", CNN's "NewsNight", CNBC's "The Big Idea", Anderson Cooper's "Anderson", and is a frequent guest on NBC.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.