Hacking the Corporate Mind: Using Social Engineering Tactics to Improve Organizational Security Acceptance

By James Philput

Abstract:

Network defenders face a wide variety of problems on a daily basis. Unfortunately, the biggest of those problems come from the very organizations that we are trying to protect. Departmental and organizational concerns are often at odds with good security practices. As information security professionals, we are good at designing solutions to protect our networks, and the data housed on them. That said, we are awful at communicating the need for these controls in a way that the users will either understand or listen to. In this presentation, we will discuss using social engineering techniques against your organization's users. Through the application of social engineering tactics, we will discuss how to bridge the gulf between the user and the information security team. Allowing for better security awareness, better adherence to information security policy, and fewer difficulties in user acceptance.

Introduction:

Information security is one of the most important and least popular departments within most companies. It is viewed as a roadblock, a compliance checkbox, a scapegoat, and a traffic cop. The information security team is the last to be brought in on a project and the first group to be blamed when something goes wrong with the organization's IT infrastructure. How have we as an industry gotten to this point? More importantly, how can we fix this? Social engineering can go a long way toward solving these problems, and improving the relationship between information security and the rest of the organization.

As Infosec professionals, we have the tools at our disposal to wreak havoc in a target organization during a penetration test. Frequently, social engineering is used as a way to show that the target company needs to seriously improve their security awareness program. In many engagements, that is where it stops. In this paper, you will learn how to extend the physical pen test model into your daily business. You will learn how to use it, not to show the organization where the security vulnerabilities are, but to change the user base's perception of the information security team.

Define the Problem:

Information security as an industry is struggling. Struggling with users who can't or won't understand why the rules are what they are. It is struggling with shrinking budgets, or budgets spent on the latest buzzword catchers by

executives with little or no knowledge of the threats faced by the organization. Most importantly it is continually struggling with uncountable adversaries bent on getting access to machines, and data that they shouldn't. Add to that the breach notifications that make the news every day, proving that organizations are leaking financial data, trade secrets, even just embarrassing memos and it points to one thing, the bad guys are winning.

The way forward lies in cooperation. Infosec staff and their users need to work together if they want to turn the tide. Unfortunately, in most organizations, the largest thing in the way of cooperation between information security staff and the users are the infosec staffers themselves. The reason being that many, if not most IT security professionals focus on what their organizations can't do rather than working to allow their user communities to help shape the workflow, and build policies that actually work for their environment. This lack of cooperation has been shown time and again in articles about the perception of IT. Over the last 12 months, articles have popped up with statements from users talking about their perceptions of IT and information security. The overriding impression that one draws from these articles is that, to the users, information security is part of the problem rather than the solution.

One of the first things that we as security professionals need to do is change our attitudes. First, stop spelling user with a leading L. The non-IT personnel in your environment are not dumb just because they don't understand computers. It is incredibly frustrating when they refuse to even try to understand. It is incredibly frustrating when they call for things that have no relation to your job. It is maddening when they blame security for problems that, you know, couldn't have been caused by anything in IT or in the security apparatus. By the same token, talk to any skilled professional, and you will find similar frustrations in dealing with people outside of their profession. Quite simply, a lack of IT/Infosec knowledge is not a crime, and the industry as a whole needs to stop treating like one.

One of the primary places that rifts develop between security staff and the organizations that they secure is in risk acceptance. Hard though it is to accept, in some cases, business need really does trump security. That said, in cases where it isn't need, but ease driving the requirement, the "trump" can be overridden. The primary argument that a business need trumps the security is that the cost of a breach is cheaper than the cost of securing the information. In absolute numbers, this is frequently correct. In reality though, the monetary damage from a breach can be significantly higher than the regulatory fees imposed by a government. Customers have been known to sue organizations that lose their information. In industries that require trust, a major breach can cause customers to move to competitors, and even cause investors to lose faith in management. The business need argument frequently stops when this cost argument is used. That said, if it continues, ask that the detailed risk assessment, and the risk acceptance by management to be given to you in writing. At a minimum this covers you in the event that the worst happens.

Remember that sometimes, there are good reasons to accept a risk. Take the time to formulate your argument before you challenge the business need argument.

In defining the problem for industry, a bleak picture begins to emerge. Organizational cooperation is poor, and the blame has been placed squarely on the shoulders of those trying to make things better, safer, and more secure. Unfortunately, unless things change, these problems are going to get worse. New technologies are continually emerging that endanger your organization's crown jewels. How can you as the ones responsible for making it work securely make the users care enough for it to matter? Trick them into it.

Define the Rules of Engagement

A challenge has been set, and you have the tools to beat it. Look at user acceptance as an objective in a penetration test. We work in an industry that prides itself on finding sneaky and innovative ways to get things that we're not supposed to have. Why not use that same ingenuity to gain support from the people that we protect? In this case, we cannot succeed in the engagement with technical skills, we will need to put on our social engineering hats, and physically interact with the targets.

The key to this engagement is the word "social". That means that the information security team must leave the comfort of their locked office and venture forth to interact with the users face to face. The team will need to study small talk, attend office functions, and generally be available to the user community. Remember, for many people outside of information security the words introverted and mean are synonymous. In order to be successful in this engagement, your security team must communicate with the users, and must do so in terms that the users will understand.

Attack!

Now that you have your social engineer's hat on, you can begin the attack. Start with a single group within the organization. Pay attention to their habits. Where do they go for lunch? What do they do during breaks? What do they talk about when they're slacking off? Pay attention to the way they speak to each other, and work on emulating it. Once you have the answers to a few of these questions, you can use that information to infiltrate the group. Find out what the group's focus is, what they need to accomplish, and use that information to formulate your security arguments, and tailor them to the target's needs.

So how do you infiltrate? To infiltrate a group, you must be able to blend in. This can be tricky for many infosec people. The problem is that the first step in blending in is appearance, and that can mean a dramatic change from the normal appearance of your information security team. You need to pay attention

to the way your target group dresses, and emulate them. This may mean moving from jeans and a t-shirt to slacks and a polo shirt. It could be more extreme and involve wearing a suit. This tends to be the biggest point of contention among information security teams, but a truly strange thing happens when the security team interacts with a user group while dressed the same way. The users begin to talk to the team as equals, and actual information can be exchanged. Stranger still, if you or your team can manage to dress better than your target group, you may be seen as authority figures.

Once you have blended in, re-examine the target. Pay close attention, not just to what they do, but how they do it. People are nearly always willing to talk about what they do to an interested peer, become one. Listen to them, find out where the group talks, and what they talk about. Get an idea of what is important to them, and never forget to use their names in conversation.

At this point, the recon phase of the attack is complete. You've learned enough about the target to blend in. If you've done things correctly, you're no longer the Security Dude(ette), you have instead become $yournamehere. In other words, you're now human in the eyes of your users. Continue speaking to them in their terms, but gradually turn the conversation to items relevant to security. Don't override the conversation, but start adding topics. Talk to them about how infosec impacts them. Explain what a breach could do to them personally. Explain what a breach in their section could do to the company. Tell them what they can do to help, and ask them to do it.

While you're talking to the users about security, don't forget to listen. Remember, at this point, you are not the infosec team dictating from on high, you are just another employee, and communication must be two-way. Find out what the users need. Listen to the stories of how security gets in the way, and examine them for inconsistencies in your policies. If you find an inconsistent policy, then it needs to be changed. From a user perspective, if one of your policies is inconsistent, then all of your policies are. Listen to what the users are complaining about and act on it when possible. If it isn't possible to change something, explain to the user why it can't be changed. Make sure to couch the explanation in terms that are relevant to the target group. Lastly, examine your policies again, and loosen any that are overly restrictive.

If your social engineering exercise was successful, you will begin to see changes in the organizational attitude. You'll get a few more requests to change processes, and policies. You will also see a more positive reception to new security policies. The key here is that the users now feel as though they have some say in what happens to them, and in how they work during their time at the office. As the users become more comfortable with the infosec people, they will become much more willing to listen to arguments brought up by the security team. The security team will be brought in at the beginning of projects rather

than the end, and you will likely start hearing more about your team in a positive light.

Lessons Learned:

First and foremost, continue the social engineering exercise. If you return to your old habits, so will your users. The second item is best summed up by a quote from Lenny Zeltser “Note to Self: They are people not users”. Remember that the people in your organization are frequently just as frustrated by you as you are by them.

The major takeaway from this engagement should be communication. A lack of communication is what has gotten many infosec geeks into trouble. Remember that your message needs to be tailored to your target audience. Pay attention to their strengths, and find ways to use those to highlight your message. Know their limitations. In this case, the limitations could be an inability to grasp information when couched in technical terms, or extreme time constraints. Remember to keep the information simple whenever possible. Don’t talk to the people as though they are children, but don’t assume a level of base knowledge that they don’t have.

In tailoring your message to a target audience, you need to consider the make-up of the audience. You will give different information to different groups. For example, different groups of managers will typically want entirely different information. When speaking to C-level executives, you need to keep your points short and easily digestible. Focus on the specific without delving into detail. Keep your points to items like spending $x will save $y, or quick statements that couch your needs in terms of regulatory requirements. Most of these executives consider their time to be too precious to expend on long presentations. A short, to the point statement or set of statements are likely to elicit a more positive response from this group than an hour long presentation on all of the merits and flaws of a particular technology.

Non-Technical management tends to be similar to the normal end users. For this group, metrics showing why x is better than y tend to be more persuasive than arguments over which specific technology to purchase. These managers can be some of your best sources of information about their groups. Their attitudes are typically reflections of their department’s attitudes. Listen to their objections in the same way you did during the main portion of the engagement. They can bring information to you that gives you a better overall picture of the workflow in their group. When presenting this group with new information, you will still need to keep things concise. They are not generally interested in the technical details, but rather in the way your changes will impact them, their employees, and the business. Once again, Regulatory requirements can be used to sway this group.

Technical management tends to be the easiest group for information security to talk to. These are the managers that teams deal with daily. Frequently, these managers act as an insulator for the security team, shielding them from the upper levels of management, and acting as the faces of the organization's information technology group. When presenting to this group, you can be significantly more detailed. Provide them with a clear definition of the problem. It frequently helps to provide technical managers with multiple potential solutions along side the problem. Be prepared to answer questions, and possibly even defend both your definition of the problem, and your proposed solution. Give these managers details, such as the likelihood of a given vulnerability being exploited. Help them to prepare to bring your findings to other groups.

Conclusions:

If you have consistently applied the techniques outlined in this paper, you should begin to see an improvement in organizational acceptance of the information security team. Remember, communication solves problems. Without clear and open dialog between the departments, the infosec team will quickly begin to lose ground, and respect in the organization. Keep your user base's limitations in mind. Explain changes to them in a way that is relevant to them. Make sure that they understand when restrictions are dictated by an outside organization such as a government entity or parent company. The most important takeaway from this presentation is that you should use what you learned from running a social engineering exercise against your organization to make security relevant to the end users. Once you have made it something that matters to them, they are significantly more likely to listen to and follow your rules.

Acknowledgments:

This paper is an original work, but I couldn't have done it without reading the articles and books below. As a group, these works provided the inspiration for this paper. Some of them take a completely different tack from what I have outlined in this paper, and advocate methods of dealing with security problems that I think would just make the problem worse. Others define the problem, without providing a solution that I liked. All of them are worth a read.

The Best Changes IT Can Make: Top 5 Reader Suggestions
By Jon Brodkin for Arstechnica

Accepting Apathy – Save Users from Themselves and You from Yourself
By Mike Rothman for Securosis

Infosec: Designing for IDGAF
By Dave Shackleford

Ghost in the Wires: My Adventures as the World's Most Wanted Hacker

By William L. Simon and Kevin D. Mitnick

The Art of Deception: Controlling the Human Element of Security
By William L. Simon and Kevin D. Mitnick

Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks
By Michal Zalewski

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
By Clifford Stoll

Little Brother
By Cory Doctorow

About the Author:

James Philput has worked in the IT industry for 15 years, and the information security sector for the last 10 years. He has worked in telecommunications, education, government, and medical industries. James is primarily network defense geek, though he has participated in several penetration testing engagements. He is currently a Sr. Information Assurance Analyst with IAP – Information Assurance professionals working to secure various client networks.