CHAPTER

8

Psychological Weapons

INFORMATION IN THIS CHAPTER

- Social Engineering Explained
- How the Military Approaches Social Engineering
- How the Military Defends Against Social Engineering

We have talked about technical attacks in Chapters 6 and 7. Now it is time to talk about using the target's behaviors to gain access to their information. Psychological Operations (PSY OPS) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals [1]. Militaries have been conducting PSY OPS, or Influence Operations, for centuries. The United States stood up Army Special Forces (Green Berets) to win the hearts and minds of the local population rather than just force to achieve victory. There has been a lot of change to doctrine based on lessons learned during operations in the Middle East, in fact the new Army FM for what was PSY OPS is now called Inform and Influence Activities and encompasses public affairs operations, military information support operations, combat camera, Soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security (OPSEC), and military deception. OPSEC and Force Protection are the defensive aspects for what we are talking about. Comparable techniques are used by Human Intelligence (HUMINT) collectors and the Intelligence Community to get enemy personnel to betray their countries by becoming spies. Similar techniques have been used in civilian society by con artists who make a living using their ability to gain someone's trust so they can take advantage of them. Many of the methods are used by salespeople to influence buyers to purchase the most expensive car. Now these techniques are being modified by hackers to get users to violate policies and common sense, thus allowing them access to critical data and are commonly referred to as Social Engineering.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00008-8

SOCIAL ENGINEERING EXPLAINED

Social Engineering (SE) is the act of influencing someone's behavior through manipulating their emotions, or gaining and betraying their trust to gain access to their system. This can be done in person, over the phone, via an email, through social media, or a variety of other methods. The difference between SE and other attacks is the vectors are through the person, or as hackers say the "wetware."

The goal of an SE attack is to create a relationship, gain the target's trust, and get them to take an action or provide some information that is a violation of their organization's policies or personal basic security practices. Some folks have the gift of gab and can do it with a cold call but most attackers will take time to prepare a story based on information known about the target. This attack vector has grown rapidly in the past few years and for some target sets is the dominant technique.

Is SE Science?

How is this science? There have been many recent publications on kinesics (the study of body and facial expressions) like Paul Ekman's books on micro-facial expressions and *What Every Body Is Saying: An Ex-FBI Agent's Guide to Speed-Reading People* by Marvin Karlins and Joe Navarro. These, combined with books on subjects like *Emotional Intelligence: Why It Can Matter More Than IQ* by Daniel Goleman, *Blink: The Power of Thinking Without Thinking* by Malcolm Gladwell, *Thinking Fast and Slow* by Kahneman, or any of the books by Dan Ariely that talk about how intuition is based on insights the person may not be consciously aware of, start to develop a body of knowledge that can be applied as a science rather than an art. These studies are developing the baseline to take this discipline from an art to a science.

This leads to the question: can SE be taught, or is it a natural ability? There is some debate on whether SE skills can be taught, but this is basically the same debate that exists for leadership, salesmanship, or any other ability. Though the arguments are often very passionate, most will agree in the end that some people have natural tendencies that make them great when they study and train in the discipline they want to master whereas others can go through the same process and only become average. So whereas some individuals will naturally become very proficient at technical hacking they may struggle to use SE techniques like the "cold call" but everyone can learn the basics and find where their talents lay. Many of the tactics, techniques, and procedures (TTPs) we will discuss are a blend of technical and SE attacks.

NOTE

The difference between SE and interrogating the person that you're trying to gain information from is interrogating is under the control of the questioner so direct questioning is the most common technique. According to Joint Pub 2-01.2, intelligence-based interrogation is the systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. The key being all techniques and methodologies undergo legal approval and review.

SE TTPs

A typical SE exploit depends on the target. There are two general scenarios: general access attacks and specific targeted access attacks. To set the stage, let's use the basic metaphor of stealing a car, keeping in mind that most metaphors when applied to cyberspace are dangerous as they don't reflect the complexity of the environment. In a general access attack, we could be looking for any car to steal. This could be relatively easy to accomplish. We could sit outside a convenience store waiting for someone to leave his/her car running and then jump in and drive away (remember to check for a baby seat) or we could use a gun and carjack someone at a light; we could go old school and learn to hotwire a car or any number of other techniques. Stealing a specific car—the mayor's car, for example—would be a different story. In the first scenario we didn't need to do any reconnaissance; now we need to put a lot of effort into recon. We have to learn what the mayor drives and figure out the best attack. We would need to understand which attack has the least chance of getting caught, as the mayor controls the police force. Depending on our motivations we may want the theft to go unnoticed for a period of time, or we may want it to be dramatic so it gets on the evening news. The same rules are true with cyber attacks but as there is an element of personal interaction in SE it is even more relevant to understand the target.

General Access Attacks

First let's look at general access attacks. These are attacks where the goal is to gain entry to any system or network. The attacker is indifferent to the owner of the system. A general phishing attack would be a good example (see note for definitions of types). The cost of sending out the emails is low; in 2010 there were about 183 billion spam emails sent a day and 2.3% were phishing attacks [2]. Compromised systems can then be used to attack other systems (making them "zombies"). Harvesting a large number of systems is useful to build systems in between the attacker and the targets. There is NO need for reconnaissance as the attacker doesn't care where the system is or what it does; they can move directly to the attack phase and, due to the low costs, accept a lower number of compromised systems.

The next example of a general attack is to release a virus. A virus is a malcode program that the user needs to run to have it work. Attackers can load a virus into a Word document, PDF, PowerPoint, picture, or even a game. These infected files will open and run (i.e., someone can open the PowerPoint document and go through the slides) at the same time the virus infects the system. The downside to an attack like this is that it can go viral (hence the name virus) and end up infecting systems it was not intended to attack. This kind of an attack can also be done with a worm which is a malcode program that doesn't need user interaction; it will infect a system and use it to infect others but this would not be a SE attack. It would be categorized as a technical attack. The proliferation of translation sites on the web and access to interesting news from the target's homeland have made this type of attack much easier to develop believable scenarios with proper grammar and cultural context that will get potential victims to take the bait.

NOTE

Standard types of attacks generally designed to steal identities:

- *Phishing*: This is where a mass email is sent to a large group of addresses (potentially millions). The email could try to lead the user to open an attachment or go to a web page, either of these actions would lead to the computer system being compromised (assuming the system in question was vulnerable).
- *Pharming*: misdirecting users to fraudulent website.
- *Spear Phishing*: This is where a specific individual is targeted and a tailored email is sent that they will open and react to. Examples would be the Sys Admin for a network or Program Manager of a target. This requires good intelligence on the target.
- *Whaling*: This is a Spear Phishing attack against the senior level of leadership of the organization being targeted.

Specific Targeted Access Attacks

Now we will analyze Specific Targeted Access Attacks. The attacker will approach the target after learning as much about them as they can via what the military calls Open Source Intelligence. Civilians would just call this "googling" someone. The attacker wants to understand the victim's interests, fears, motivations, attitudes, and desires. This will allow the attacker to tailor the attack and increase the chances of success. Key information includes knowledge of significant dates (birth, marriage, etc.), addresses, phone numbers, family members, interests, relationships, photographs, and work and education histories. If the target is active on social networking sites this is a great place to start; the greater their electronic footprint the better. There are many places to learn about the target:

- Personal info can be found on social media sites like Facebook or MySpace (this includes relationships, activities like sports, volunteering, religious practices, political beliefs, and so on)
- Professional information is on networking sites like LinkedIn or job sites like Monster (this also tells you what they are working on)
- Geolocation info on sites like Google Earth or location-based services like Foursquare
- Financial information like tax records and home ownership records
- What they are thinking can be read on via their Twitter pages or blogs
- Involvement in virtual worlds like Second Life or gaming site (where people can meet as any avatar they create)
- Membership info from organizations like academic alumni, clubs, professional organizations, or hobbies

TIP

Privacy has different meanings to individuals based on their generation and the culture they were raised in. For many of the younger generation who have been raised with computers (sometimes called Digital Natives) they have a large part of their lives online, to the point some have their

diaries as part of their public web pages. Their expectations of privacy are different than most of the folks running the militaries and intelligence communities today. These digital natives can become vectors for attack if they have relationships with someone that has been targeted. It is important that everyone understand what is being posted and what is acceptable.

Types of SE Approaches

Once the attacker has gathered the background information necessary to understand some options to approach the target they must decide how aggressive they want to be. From least to most aggressive the approaches are: observation, conversation, interview, interrogation, and torture. They can start by digital or physical observation. Next comes a conversation (electronic, telephonic, or in person). This is often the phase where the attacker will determine who they want to recruit or attack. Typically this is known as elicitation which is generally the extraction of information through what seems to be a casual conversation. To phrase this another way it is "where the con is based on the social engineer's" ability to spin a lie. This ability comes from pretexting which is developing a scenario where the SE gains the trust of the person who owns or has access to the information in order to get them to break their policies or violate common sense and give the information to the attacker. One method that is used in every type of attack but is especially useful here is mirroring. For example by adopting the target's speech mannerism (or email style) it will be much easier to get them to engage in a conversation.

WARNING

The Financial Modernization Act of 1999 more commonly known as the Gramm-Leach-Bliley Act makes pretexting a crime. Under federal law it's illegal for anyone to [3]:

- Use false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious, or fraudulent statements or using false, fictitious, or fraudulent documents or forged, counterfeit, lost, or stolen documents.
- The Federal Trade Commission Act also generally prohibits pretexting for sensitive consumer information.

The next technique is to conduct an interview or outright interrogation. Both of these require the victim to submit to the attacker's authority. This can be done by posing as a customer who needs the information to make a decision, pretending to be someone from the government who has the right to the information, or through intimidation. These attacks can be done cold or after a relationship has been developed. The attacker can perform them in person using props like badges or over the phone/email using spoofing to make it appear like the

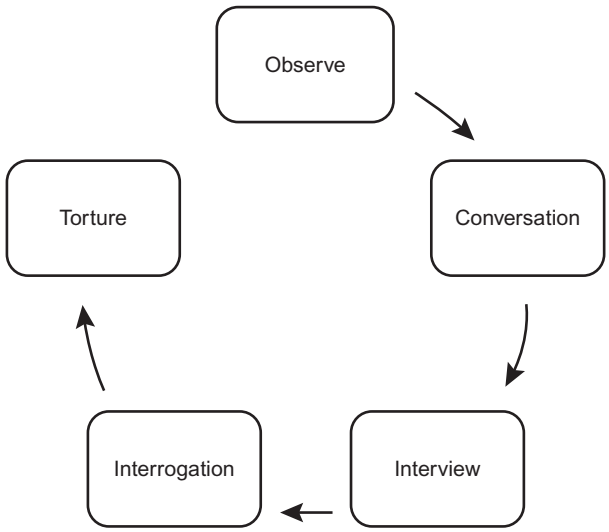

FIGURE 8.1 Approach techniques from least to most aggressive.

contact is from a legitimate source. An example would be to call someone as the Tech Department or Help Desk and tell them they have to reset their account because of a mistake made during a recent update. Most people want to be helpful and automatically trust their computer. That desire to help or trust in their system is the key to compromising them. Both of these techniques are not by their nature antagonistic. Often the most effective techniques are based on establishing common bonds. All of these techniques require building a relationship based on trust. Finally, after interrogation comes torture, but that is beyond SE practices. Figure 8.1 shows the flow of these Techniques.

Types of SE Methodologies

Some typical methodologies for general collection are divided into physical and electronic. Physical techniques include things like: dumpster diving (digging through target's trash), shoulder surfing (looking at a target's screen or keyboard while she/he works), observation (tracking a target's activities—think stakeout), spy gear (like directional microphones/hidden cameras), and impersonation (posing as utility worker). Electronic techniques include: open web search (using all the features of a search engine—i.e., Google will just search blogs), Pay for Service sites like Intelius or U.S. Search, Credit Information Requests, social networking site searches, and professional networking site searches and geolocation sites (e.g., Google Street View).

Though this information is generally openly available the social engineer may need some tools to make the research more effective. These include web sites and tools like:

- SE Toolkit (technical hacks against the user)
- American Registry for Internet Numbers (IPs and phone numbers for North America)
- Freedom of Information Act requests

- Social media—OpenBook (Facebook searches), LinkedIn, Friendster, Monster, Yelp, Craigslist, Jigsaw, FriendFinder, PiPI, Plaxo, wordpress, Shodan
- Maltego and Maltego Mesh (link mapping)
- BeEF (webpage redirection)
- TwitScoop and Tweepz (Twitter searches)
- Creepy [http://ilektrojohn.github.io/creepy/] and TwitterMap (geolocation)
- Edgar [www.sec.gov/edgar] (corporate info)
- Sites like Spokeo (people search) and Telespoof.com (caller ID spoofing)

Additional tactics include:

- Camouflage
  - Fake business cards, disguises (facial or uniforms), and fake or cloned badges
  - Props (everything from clipboards to toolkits to deliveries)
- Lock Picking/Tailgating
- Cameras/hacking into video system
- GPS tracker

This is just a quick list of some of the different types of tools that can be employed as part of SE.

One recent event that has captured the media's attention was the SE Capture the Flag (CTF) event at the 2012 DEFCON 20 called "The Battle of the Sexes." There has always been a network-based CTF event but in 2010 DEFCON started SE CTF. The latest competition is an evolution to compare results based on gender (women captured more flags). There have also been competitions for youth to train the next generation. Here is an excerpt from the report on the event:

> Contestants were assigned a target company, with each having two weeks to use passive information gathering techniques to build a profile. No direct contact between the contestant and the target was allowed during this time. The information was compiled into a dossier that was turned in and graded as part of the contestant's score. During DefCon, contestants were then allowed 25 min to call their target and collect as many flags as possible, which made up the remainder of their score. Flags were picked to be non-sensitive information, and each was assigned a point value based on the degree of difficulty in obtaining the information associated with the flag. A few examples of the 25 flags are: In House IT Support, New Hire Process, Anti-Virus Used, Is there a Cafeteria, Wireless On-Site, Badges for Bldg Access and What OS Used.
>
> Complex searches lead the contestants to gather quite a few PDFs or web pages that answered each of their inquires in full detail. One interesting surprise was the use of Google Street View as an information gathering tool. A primary factor in the success or failure of the contestant was the planning of the overall attack. The most interesting aspect of this has to do with how quickly and easily information could be obtained from all companies in a relatively short period of time, even with the caller under pressure. Final results were 15 companies called and 14 of them had flags captured [4].

HOW THE MILITARY APPROACHES SE

The military has been in the spy-counterspy business from the beginning; they are also experts at interrogation. Spying is the long con, whereas interrogation is generally the method used to get access to information in an immediate situation. This section will focus on the near

term gathering of data (or the short con). We will look at the techniques used to extract information and discuss how they apply to SE.

First, we must understand that these techniques have been developed to work in both peacetime operations and combat situations. They are normally done in a controlled environment and are very similar to the techniques used by law enforcement agencies. The basic principles are similar to SE and the foundational principles and many of the techniques apply well to SE attacks. The military trains interrogators that stay in that discipline their entire careers. They become proficient in the languages and culture of their assigned region. HUMINT operators or interrogators are trained to deal with screening refugees, debriefing U.S. and allied forces, interrogating prisoners of war, interviewing collaborators, exploiting captured material, liaising with host nation, acting as interpreters if needed, and interacting with the local population.

Army Doctrine

We will discuss how the army deals with interrogation as they are the ones who are on the ground dealing with these issues. The basic techniques we will cover are from "FM 2–22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS" September 2006 [5].

Goal: collector's objective during this phase is to establish a relationship with the source that results in the source providing accurate and reliable information in response to the HUMINT collector's questions.

Key principles: From a psychological standpoint, the HUMINT collector must be cognizant of the following behaviors:

- Want to talk when they are under stress and respond to kindness and understanding during trying circumstances.
- Show deference when confronted by superior authority.
- Operate within a framework of personal and culturally derived values.
- Respond to physical and, more importantly, emotional self-interest.
- Fail to apply or remember lessons they may have been taught regarding security if confronted with a disorganized or strange situation.
- Be more willing to discuss a topic about which the HUMINT collector demonstrates identical or related experience or knowledge.
- Appreciate flattery and exoneration from guilt.
- Attach less importance to a topic if it is treated routinely by the HUMINT collector.
- Resent having someone or something they respect belittled, especially by someone they dislike.

These principles are used to develop an approach, build rapport, and establish a relationship in which the HUMINT collector presents a realistic persona designed to evoke cooperation from the source. In the military things are usually done in accordance with established procedures and if it is a mission (like an interrogation) should have a documented plan. This is not to say soldiers are not flexible and resist innovation but rather to say they want to increase the chances of mission accomplishment and have found these lead to greater success. The HUMINT collector must ensure their body language and personal representation match their approach.

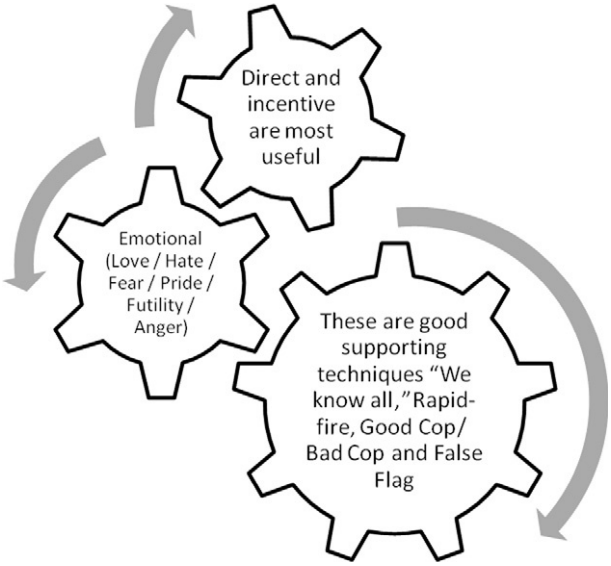

FIGURE 8.2 The various approaches must be integrated.

Some standard operating approach techniques are: direct, incentive, emotional (Love/Hate/Fear/Pride/Futility/Anger), "we know all" or "file/dossier," rapid-fire (don't let them talk), Mutt and Jeff or good cop/bad cop, and false flag (misrepresentation of oneself). See Figure 8.2 for how these relate to each other. The direct approach is simple and straightforward. It is simply telling the person what they want and using interview/interrogation skills to convince them to cooperate and share the information. This technique is useful in a conventional war but not very useful in counterinsurgencies or for SE. Statistics from interrogation operations in World War II show that the direct approach was effective 90% of the time. In Vietnam and in Operations URGENT FURY (Grenada, 1983), JUST CAUSE (Panama, 1989), and DESERT STORM (Kuwait and Iraq, 1991), the direct approach was 95% effective. The effectiveness of the direct approach in Operations ENDURING FREEDOM (Afghanistan, 2001-2002) and IRAQI FREEDOM (Iraq, 2003) is still being studied; however, unofficial studies indicate that in these operations, the direct approach has been dramatically less successful [5]. The military is still analyzing the reasons but one common assumption is that the motivations of religious fanaticism are harder to compromise than traditional nationalism. There are some general types of direct questions that are useful: Initial (get the discussion going), Topical (focused on establishing how much they will communicate and what their level of knowledge is), Follow-up (making sure we have gained all the primary and peripheral information), Nonpertinent (establishing rapport and keeping discussion going), Repeat (seeing if they are consistent), Control (establish baseline), Prepared (for areas interviewer is unfamiliar with or highly technical topics). One of the key questions here is the control or baseline question. It establishes how someone behaves when they are telling the truth. Much like a polygraph test that starts with baseline questions like name and address then gradually that builds to questions related to guilty actions to compare stress reactions against, a social engineer must understand how the target behaves when not under stress.

The indirect approach, or using elicitation, can often be useful as we combine information gathering from normal conversations with targets of interest without them knowing they are being interrogated. Elicitation is a sophisticated technique used when conventional collection techniques cannot be used effectively. Of all the collection methods, this one is the least obvious. However, it is important to note that elicitation is a planned, systematic process that requires careful preparation [5]. This is where the more the interviewer knows about the target the better, so they can have a natural flowing conversation. For example, they may start by sharing information they have so the target assumes they know all about it and will openly discuss the details.

Next comes incentive. This is basically offering the target something they want or need. The first thing that comes to mind is bribing them, but it can be as simple as an email offering to increase their speed or access to the Internet. This approach can be very effective when tied to the right emotions. The emotional approach is where the target's emotions are brought into the interaction to get them to take an action that they would not normally do. A recent example of this is what is known as scareware. A good example is when a pop-up box announces there is a problem on the user's system that can be fixed by installing a free update. In reality this scareware update is a Trojan horse whose only function is to compromise the user's system. This approach is based on Fear, other emotions that can be used are: Love (in its many forms), Hate or Anger (us against them), Pride (in themselves or their organization), and Futility (there is no other option). Picking the right emotion is easier in person because we can read the body language or on the phone where we can judge the tone of voice and modify the approach based on the situation. The goal of this method is to manipulate the target's emotions so they override their natural cognitive reactions.

Other well-known techniques are: "we know all" or "file/dossier"; this is where the interrogator comes in and lays a folder labeled "witness statements" or a DVD labeled "surveillance footage" on the desk. This fake evidence contains no actual information but allows the interrogator to start by saying something like, "we have the evidence we need but want to get your side of the story before we submit our final report." For a social engineer/interrogator the presentation of material that supports the belief that the interrogator knows the basics but just needs the target to provide the details. If target is still not talking freely it may be time to try the rapid-fire method where the interrogator keeps interrupting the target so they get frustrated and jump in with key facts so we will listen. The rapid-fire method is also used when the target is going to tell a lie that the interrogator doesn't want them to say like "I have never been to that site" because once they tell a lie they are committed to it. To get to the truth we first must make the target to admit they lied.

The last two methods we will discuss are Mutt and Jeff, or good cop/bad cop, and false flag. We have all seen the aggressive and compassionate interview team in movies. The target will identify with the compassionate person and tell their story so the good cop will shield them from the aggressive cop. This method can also be modified so a really abusive interrogator is followed by one who apologizes for the unprofessional behavior of their colleague. Typically the good cop would help the target rationalize their actions so they can talk openly. One way this method can be used by social engineers is on social networking sites; we could present a Fakebook (fake FaceBook) personality created for the attack as a cyber bully and a second as someone defending the target.

Finally using the false flag, for the military this might be having a new interrogator come in and pretend to be from a friendly country or a nongovernment origination like the Red Cross. This is very useful as it is simply misrepresentation and is a bedrock of SE.

We can see that most of the techniques used by the military are directly applicable to the civilian sector and can be applied to both physical and cyber environments. The most important aspects the military brings are proven TTPs and careful mission preparation and planning. These when applied to SE will give the attacker a strong capability to be successful on their mission.

HOW THE MILITARY DEFENDS AGAINST SE

As discussed earlier, the military has been in the spy-counterspy business from the beginning. The counterspy techniques are the same skills needed to defend against SE. Today's solider needs to understand counterintelligence (CI), counterterrorism, force protection, and Operational Security (OPSEC) techniques. This section will focus on the tactical level actions that can be done for CI. First let's review the doctrinal definitions for the key concepts:

- CI: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities [6].
- Cyber CI: Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions [6].
- Counterespionage: That aspect of CI designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities [6].
- Counterterrorism: Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks [6].
- Force Protection: Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease [6].
- OPSEC: A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems; (b) determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation [6].

The military depends on confidentiality and secrecy. They deploy encryption, data classification, clearances for their personnel, and a thorough set of processes and regulations. Soldiers, airmen, seamen, and marines understand the trust they have been given and the level of national security compromise that could occur (not necessarily through a single loss of data but the aggregate knowledge impact as well). Cybersecurity has become a critical component of the National Counterintelligence Strategy (see Figure 8.3). The mission to secure the nation against foreign espionage and electronic penetration of the IC, DoD, and to protect U.S. economic advantage, trade secrets, and know-how is becoming a core responsibility for the military.

CI has an offensive aspect as well. There is a need to set up internal traps or as they are called in cyberspace "honey pots" to attract insiders accessing information they are not authorized for. These honey pots will also capture outside threats that have gained access. Another technique organizations should consider is to have enticing files with embedded beacons that report back on where they end up when stolen to provide situational awareness on what has leaked out and who did it. Organizations need to fund programs to gain access to

FIGURE 8.3 Counterintelligence is a national concern; this is the U.S. strategy to deal with it [7].

the types of organizations that have the motives and means to attack the United States and see what they have stolen. Organizations need to conduct exercises and tests on our personnel to assess our readiness level. Finally, we need to enforce consequences on individuals caught violating policies.

How the Army Does CI

Army regulation (AR 381-12 Threat Awareness and Reporting Program 4 October 2010 (for the old soldiers this was called Subversion and Espionage Directed against the U.S. Army or SAEDA)) establishes the training requirements and reporting procedures. It also lays out indicators or suspicious activities, such as foreign influence or connections, disregard for security practices, unusual work behavior, financial matters, foreign travel, undue interest, soliciting others, and extremist activity. This is basically a process that encourages every member of the staff to become a security officer and help police both themselves and their coworkers. The program is built around two key principles: situational awareness and behavior monitoring, both for themselves and their coworkers. If done well, it will counter the whole spectrum of crime, internal threats (disgruntled or unstable workers), external threats (foreign operatives and terrorist), and today's social engineers. If done poorly, it allows incidents like the recent unauthorized release of a large number of classified documents relating to the U.S. war in Iraq to WikiLeaks to occur.

An Air Force Approach

The Air Force Public Affairs Agency has published a "Social Media Guide." Top 16 tips include items like: differentiate between opinion and official information and no classified information [8]. This is a very good example as it does a couple of things well. First the guide is more about what we should use rather than why we should not use the many different communication applications on the web. Second it is a formal policy that includes punitive consequences for misbehavior.

An important aspect of this defensive capability is to analyze the information that is leaking and conduct the appropriate investigation to determine what actions need to be taken. Historically there are examples of traditional espionage like Aldrich Ames, Robert Hanssen, Colonel Vladimir Vetrov, a KGB defector known as the Farewell Dossier, Gregg Bergersen, and the 11 Russian spies recently deported from the United States, but these operations are time consuming, expensive, and risky where we can get much of the same material through cyber spying. The risk of getting caught is lower, the time to gain access is faster, and the cost is cheaper. We have talked extensively about computer network exploitation; when we combine that with SE we have a paradigm shift in spying capabilities. This requires us to look at the techniques that got these traditional spies caught, including careful analysis, auditing financial records, tips from co-workers, offensive operations to gain access to enemy files to see who they had turned into spies, and encouraging defectors to switch sides.

For the sake of brevity, we're not going to delve into the processes of the Navy and Marine Corps, although they're both quite capable in their own right at these processes and procedures.

SUMMARY

SE is a very dangerous threat vector to all organizations and individuals. It requires training and vigilance to defend against. For example, a simple questionnaire sent to a target on a social networking site asking the target to answer question about themselves so they can become closer friends could include the same questions asked by the company to reset the target's password and now the target's organization is compromised. We need to make sure people are vigilant and cautious (remember you're not paranoid if they are out to get you). We can leverage lessons learned in the military to understand how these SE attacks work and how we defend ourselves. Defenses against SE must be focused on behaviors.

The policies, culture, and training must be reinforced often to insure the workforce stays vigilant. Training the staff to have situational awareness is key to a good counter-SE program. This training must be continuous with messages from multiple sources—emails, meetings, and formal training. There need to be exercises to test the staff like emails asking employees to go to a site and enter their password only to find a message from the company that they would have allowed hackers to gain access to the network if it was a real attack. Security audits should include SE attacks to validate that the training is effective. There is a saying in the hacker community: "You can't patch stupid," which often refers to the fact that if an organization has a great technical security infrastructure and the attacker could not penetrate them, just go after the people. People are not stupid; they just don't understand the risks they are taking with their actions. Training is a critical step to fixing this threat vector.

The bottom line is: this is the growth area for threat vectors via social media and the only way to defend against it is executive awareness, user training, and validation exercises.

References

[1] Department of Defense. Joint electronic library, http://www.dtic.mil/doctrine/ [accessed 17.01.13].
[2] Commtouch Software Ltd Q1 2010 internet threats trend report, http://www.commtouch.com/press-releases/well-known-web-names-misused-to-give-spam-deceptive-legitimacy-according-to-new-report-by-commtouch/ [accessed 17.01.13].
[3] Financial Modernization Act of 1999. Federal Trade Commission. Facts for consumers, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre10.shtm [accessed 17.01.13].
[4] Hadnagy CJ, Aharoni M, O'Gorman J. Defcon 20 social engineering CTF, http://www.social-engineer.org/social-engineering-ctf-battle-of-the-sexes [accessed 17.01.13].
[5] Army, U.S. FM 2–22.3 (FM 34–52) Human intelligence collector operations. Public affairs, https://www.fas.org/irp/doddir/army/fm2-22-3.pdf; 2006 [accessed 17.01.13].
[6] JP 1–02 from Department of defense. Joint electronic library, http://www.dtic.mil/doctrine/ [accessed 17.01.13].
[7] Office of the director of national intelligence's office of the national counterintelligence executive, http://www.ncix.gov/publications/strategy/docs/2008_Strategy.pdf [accessed 17.01.13].
[8] Air force social media guide 2012, http://www.af.mil/shared/media/document/AFD-120327-048.pdf [accessed 17.01.13].