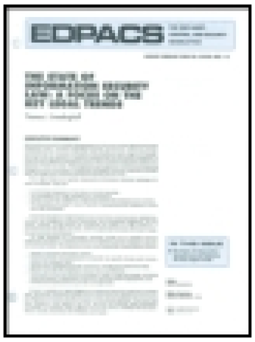

EDPAC: The EDP Audit, Control, and Security Newsletter

ISSN: 0736-6981 (Print) 1936-1009 (Online) Journal homepage: www.tandfonline.com/journals/uedp20

Social Engineering Techniques, Risks, and Controls

Gary Hinson

EDPACS THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

APRIL–MAY 2008 VOL. XXXVII, NOS. 4–5

SOCIAL ENGINEERING TECHNIQUES, RISKS, AND CONTROLS

GARY HINSON

SUMMARY

This article describes typical social engineering threat sources and techniques, analyzes the associated information security risks, and outlines a range of preventive, detective, and corrective controls to minimize social engineering risks.

BACKGROUND

Social engineering involves the use of social skills to manipulate people in order to obtain unauthorized access to information assets. “Social engineering is a form of hacking that relies on influencing, deceiving, or psychologically manipulating unwitting people to comply with a request” (Mitnick, 2006). “Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim” (Wikipedia, 2008). “To attack your organization, social engineering hackers exploit the credulity, laziness, good manners, or even enthusiasm of your staff. Therefore it is difficult to defend against a socially engineered attack, because the targets may not realize that they have been duped, or may prefer not to admit it to other people. The goals of a social engineering hacker—someone who tries to gain unauthorized access to your computer systems—are similar to those of any other hacker: they want your company’s money, information, or IT resources” (Microsoft, 2006).

Social engineering is a cross between acting, fraud, and hacking, combining psychological tricks with sheer bravado, typically to manipulate people into giving unauthorized access to information and systems/networks. Social engineers are skilled at putting on a show, a convincing act to persuade the “mark” (their target) to give up sensitive information, perhaps run a key-logger program, or simply let them enter the office and wander about. Like confidence tricksters and fraudsters generally, social engineers take

IN THIS ISSUE

Taylor & Francis
Taylor & Francis Group

advantage of human gullibility. They have the nerve to tell barefaced lies and the credibility to build (misplaced) trust. Whether it's an Oscar-winning performance or a pantomime act, the unfortunate fact is that a good proportion of these attacks are likely to succeed, especially in a typical corporate environment where employees implicitly trust those who they believe are fellow employees. "Trusted people can even inadvertently help attackers. They are particularly vulnerable to attackers pretending to be other trusted people, either on the phone or in person and wearing the correct uniforms. For example, building guards can be fooled by an attacker wearing an appropriate uniform; guards have even been known to help properly dressed criminals carry stolen goods out of the building. Computer users can be fooled by someone pretending to be from their company's tech support office" (Schneier, 2003, p. 143).

In a corporate context, social engineering is a factor in most information security incidents, including (perhaps especially) those perpetrated by insiders. Employees have plenty of opportunities to use social engineering techniques, often under the guise of casual inquiries or even jokes ("Oh go on—I bet your password is something easy to guess like your dog's name …"). Employees are actively encouraged to call the IT Help Desk (or IT Service Desk for ITIL users) for technical assistance and of course the Help Desk workers are trained to be helpful. "Pretext calls" made by employees can be particularly convincing as they have ready access to vast amounts of internal information to build their credibility and make the pretext sound convincing. They can browse the intranet telephone directory and structure charts to pick suitable targets. Picking up the name of sensitive systems and projects is a breeze for insiders. We all know how effective "clear desk and clear screen" policies are in practice. We even provide telephones, photocopiers, FAX machines, and e-mail facilities to make their lives that bit easier!

Social engineering attacks also work on a personal level. 419 (advance fee fraud) and phishing scammers, for example, exploit gullible victims who fall for lures such as the promise of a huge legacy/lottery win or the need to "update their personal information" held by the bank (Hitchcock, 2006; Lininger & Vines, 2005). Victims who are fooled into believing the scammers' stories are manipulated into disclosing personal information and handing over money, either directly or as the result of subsequent identity theft.

SOCIAL ENGINEERING RISKS

To hackers, industrial spies, private investigators, journalists, and others, social engineering is a highly attractive method of gaining access to sensitive and valuable information. It is an effective and low-risk alternative to conventional hacking (technical network/system penetration) methods. What's more, almost anyone is potentially capable of mounting a social engineering attack: the basic skills are commonplace and frequently practiced. Some people have a natural flair for it, others simply learn as they go. The very best make a profession of it and are so good that their targets seldom even appreciate they have been "had" (Winkler, 2005).

To understand the social engineering risk in more detail, I will break the topic down into its constituent parts—threats, vulnerabilities, and impacts—because social engineering risks necessarily involve the congruence of all three factors.

SOCIAL ENGINEERING THREATS

Because social engineering as a whole is a threat, this analysis concentrates on characterizing the "threat sources," namely those who socially engineer others.

In the extreme, practically all of us could be classified as social engineers. Human social interaction naturally involves communicating with others and often persuading them to do something we want them to do. Professions such as sales and teaching develop the skills, whereas fraudsters and con-artists abuse essentially the same skills. Social engineers span the borderline between legitimate and illegitimate use of the techniques, exploiting that ambiguity through questions and statements that *could* be totally innocuous. "Penetrating a company's security often starts with the bad guy obtaining some piece of information or some document that seems so innocent, so everyday and unimportant, that most people in the organization wouldn't see any reason why the item should be protected and restricted" (Mitnick & Simon, 2002, p. 15).

Although we normally think of social engineers like hackers as self-motivated loners or members of small close-knit teams, there is evidence that organized criminals and even state-sponsored espionage activities sometimes employ social engineering methods. "Shell is understood to have uncovered a 'special interest group' in Houston consisting of its Chinese nationals, who were encouraged to meet socially after work. The networking group was, however, 'a front for recruiting Chinese nationals'. In what security experts described as a typical form of 'social engineering', there was targeting of Chinese workers whose families were still in China. They were told to help 'for the good of the Motherland', the source said, adding: 'It was a form of threat. This particular European oil company was made aware and uncovered the spying operation, where the Chinese were put under moral pressure to give information'" (Rossiter, 2007).

Like pushy sales representatives, social engineers can be assertive and manipulative. "The social engineer maneuvers his or her target into an alternative rôle, such as forcing submission by being aggressive" (Mitnick & Simon, 2005, p. 234). They are not averse to telling lies using a method known as "pretexting." "Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is typically done over the telephone. It's more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target" (Wikipedia, 2008).

At the risk of over-generalizing, social engineers typically:

□ Are unethical, skilled, and well-practiced fraudsters and liars, able to put on a convincing act, for example, appearing to be

fellow employees, maintenance engineers, researchers, journalists, managers from another office, suppliers, partners, customers, prospects, IT system administrators, IT Help Desk workers, the police or family members;
□ May be self-motivated or may be working for a third party;
□ Deliberately blend-in to their surroundings so as not to attract attention (e.g., by “tailgating”—following an employee in through an access controlled door without needing a pass);
□ Claim a legitimate reason why they need access to the information and/or the facilities;
□ Choose appropriate contact methods (e.g., telephone calls, emails, physical visits, websites such as Facebook);
□ Present false e-mail addresses, identity cards, business cards, headed notepaper, or various other credentials (e.g., company overalls, sign-painted vehicles, name-dropping) to support their fake identities;
□ Gather and correlate information from a variety of sources (e.g., published on the Web, stolen from garbage bins), gradually establishing knowledge of the target to appear more credible and identify potential vulnerabilities;
□ Tell lies, flirt with, cajole, or threaten people into revealing information;
□ Build rapport with their targets so as to appear trustworthy and legitimate, for example, by offering gifts or help with technical problems (that they might have engineered in the first place);
□ Are very persistent, much like unwelcome sales representatives or genuine spies—in extreme circumstances (if the potential prize makes it worthwhile) they may spend weeks, months, or even longer cultivating relationships and building their credibility;
□ Are quite systematic, dedicated, and focused in their approach;
□ Work alone but may form small tight-knit teams when the advantages of collaboration outweigh the additional risks of detection or betrayal.

A social engineer’s key skills or traits therefore include:

□ The ability to persuade, coerce or manipulate other people;
□ Credibility and empathy—useful for lying convincingly and establishing trust, getting people to open up and reveal information casually, for example, by flattering them or flirting;
□ Confidence, bravado, and assertiveness, coupled with the experience to know when to push and when to let up;
□ Being good at listening, remembering, correlating, and using useful snippets of information;
□ Focus and single-mindedness, able to concentrate on the matter in hand and persist until the goal is attained.

It could be argued that these same skills are beneficial to professions such as acting, journalism, politics, and maybe even management in general. Like many other personal skills, social engineering can be improved through practice. Virtually any situation where one has the opportunity to “get information out of someone” is a chance to try social engineering. There are training courses and books on it too, albeit under more socially acceptable titles such as sales negotiation. Teachers, security awareness experts, and sales representatives all rely heavily on social engineering skills, albeit they would best be classed as white hats.

Enterprising social engineers sometimes combine their normal deceptive/manipulative people-focused techniques with other methods such as computer hacking and physical site penetration (sometimes called "blended attacks") or they may work with experts in these other disciplines (Mitnick & Simon, 2002; Winkler, 2005). For example, they might persuade a target to install a keyboard logger, whether a Trojan horse program or even a hardware memory device inserted into the keyboard lead, under the guise of needing to diagnose or solve a common computer problem. Social engineering is a powerful adjunct to many hacking techniques, particularly if the technical security controls are strong, thus limiting the scope for conventional hacks. Other examples are:

□ Installation of network analyzers, bugs, and other surveillance devices on corporate facilities;
□ Interception of wireless communications including wireless LANs, Bluetooth connections, and, potentially at least, point-to-point microwave network links;
□ Manipulating phone and computer systems to conceal their true identity and location;
□ Misuse of corporate voicemail and e-mail systems to send messages that appear to confirm the attacker's origin, or to accept reverse charge calls to the company;
□ Convincing employees to disable or remove technical or physical access controls, disclose passwords, hand-over passes or keys, and so on, perhaps under the guise of offering "technical support" or "for testing."

SOCIAL ENGINEERING VULNERABILITIES

Social engineering attacks play directly on the most vulnerable part of our information security control systems: you and me, the people (Mitnick & Simon, 2002; Winkler, 2005). Computer systems *can* sometimes be misled by people or other computer systems but once in place, properly configured, used and managed technical security measures (such as cryptographic authentication) are generally quite reliable and effective controls. The same unfortunately cannot be said of those who specify, build, use, and manage them. We, the people, are usually the least reliable parts of the control system. "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems" (Schneier, 2000, p. 255).

Psychological traits of the victims are the main reason that social engineering attacks succeed. People generally like being helpful and mostly avoid confrontation. We have a natural tendency to trust other people, especially those who have an inherent air of authority or trustworthiness. "In its most common form, the social engineer puts his or her target into the role of helper. Once a person has accepted the helper role he or she will usually find it awkward or difficult to back off from helping. . . . Helping can make us feel good about ourselves. Social engineers find many ways of taking advantage of our inclination to be helpful" (Mitnick & Simon, 2005, p. 234). We are also quite lazy when it comes to verifying things—we take too much at face value. Think for example about the common policy for employees to challenge unrecognized and unescorted visitors in "secure" areas: this is seldom very effective in practice because employees are reluctant to stop and question visitors and/or are "too busy" to check their credentials. In most cases, they are more likely to hold the door open to an unknown visitor than to ask to see a security pass.

Placing excessive trust in authority figures is a particular problem for strongly hierarchical organizations. Soldiers and policemen are no longer trained like robots "to act, not think" but still respond almost instinctively to commands from a senior officer, or to someone claiming the authority of a more senior position. Social engineers sometimes play on this by referring to senior people by rôle and/or name to add weight to their demands for information ("Hurry up man—the Chief Executive is waiting for the list!"). Inexperienced, junior, or naïve employees are more vulnerable to such techniques.

People who appear to be "insiders" or colleagues automatically engender a greater level of trust than those who are clearly strangers. Social engineers typically spend time researching their marks, systematically gathering background information and terminology to build credibility as trusted insiders. What better guise than "I'm calling from IT regarding your network access problem . . .," especially if the social engineer has somehow created or pointed out the very issue they are offering to solve.

Social engineering attacks of that nature hint at another vulnerability: employees seldom appreciate the possible significance of seemingly trivial individual items of information such as the names of people or systems. Social engineers collect and collate information from multiple sources to build the bigger picture. There is a positive feedback loop here because the more insider information they possess, the easier it is to fool other employees into revealing yet more information. A typical illustration of this issue is the widespread use of "out of office" messages on e-mail or voicemail systems. It is commonplace for people to give the names and telephone numbers or e-mail addresses of colleagues who are "dealing with urgent issues" while they are away on holiday or on business. It may be quite straightforward for a social engineer to harvest this kind of information from spam messages without the need to obtain the corporate phone directory (which is of course another technique).

"Dumpster diving" relies on people thoughtlessly discarding information into the trash, or for that matter into an insecure "confidential waste" bin (surely a honeypot for social engineers who physically penetrate the workplaces or homes of their victims, or if bins are left at the roadside). "Business paper waste can contain information that is of immediate benefit to a hacker, such as discarded account numbers and user IDs, or can serve as background information, for example telephone lists and organization charts. This latter type of information is invaluable to a social engineering hacker, because it makes him or her appear credible when launching an attack" (Microsoft, 2006).

Studies have demonstrated that computer disks are sometimes sold or disposed of with the same disregard for security. Basic tools are readily available to undelete data or unformat disks or indeed whole systems that have not been securely erased. Professional adversaries have access to more powerful forensic tools and techniques, if needed.

Yet another source of vulnerability arises from corporate functions whose very rôle is to divulge information. Public Relations and Sales and Marketing, for example, routinely publish information. Human Resources often disclose details about technologies and IT systems in vacancy notices, and reveal even more through agencies and in job interviews. Social engineers, not just customers and business partners, value information published on corporate websites and in the right hands, Google makes a wonderful hacking tool. Persuading these people to consider the possible security ramifications is one of the Information Security Manager's tougher assignments.

SOCIAL ENGINEERING IMPACTS

From an information security perspective, loss of confidentiality is perhaps the most common immediate impact of social engineering attacks. The whole point of confidentiality, clearly, is that certain information ("secrets") should only be disclosed to a limited number of individuals. Social engineering is a powerful technique for gaining unauthorized access to confidential proprietary or personal information.

Examples of the types of information that would be valued by social engineers are:

□ Miscellaneous trivia used to establish their own credibility as insiders or authority figures, for example, the lingo, abbreviations, and slang, perhaps even casual gossip and rumors. Staff working in bars and shops near your corporate HQ probably have a fair idea about what your organization is up to, even if you work for the FBI or NSA;

□ Internal procedures, for example, how visitors and employees are authenticated, who has the ability to change firewall security configurations, and so on;

□ Phone/e-mail directories, organizational structure charts, and maps showing physical building layouts or network diagrams;

□ IT-related items such as system names and types, passwords/PIN codes, network protocols, software versions, and so on—these are classic objectives for computer hackers;

□ Corporate secrets—the ultimate goal of an industrial espionage attack is typically to obtain details of R&D projects, marketing plans, strategies, pre-publication financial reports, internal management reports, and so on from the target company;

□ Personal information about the private lives of individual employees, customers, and so on that might be used in alimony cases or for coercion and fraud such as identity theft.

Loss of integrity is a lesser impact of social engineering in the sense that the integrity of the organization's security and control framework may be called into question as the indirect result of a successful social engineering attack. Someone who realizes they have been duped is perhaps more likely to doubt the integrity of subsequent callers and may be unduly reluctant to impart useful information even to colleagues with a legitimate need-to-know. On a wider scale, reticence to release information without authenticating the requestor reduces the organization's general efficiency as well as reducing the risk of unauthorized disclosure. Paranoia and introversion are not characteristics commonly associated with the most successful sales or Help Desk people!

Loss of systems or data availability may be a further secondary impact if the social engineers subsequently hack in.

From a commercial perspective, social engineering attacks may cause significant financial losses. A competitor who obtains proprietary information about a secret production process, for example, might be able to duplicate the victim's products directly, or at least erode the competitive advantage. In the case of, say, a financial institution, public disclosure of the fact that sensitive information had been stolen would damage the organization's image and probably its share price, adding to the direct loss.

Finally, there is the personal perspective. How would you feel if, say, an old flame were to find out about your private life and personal finances? Or if your identity was stolen and used to obtain credit in your name? What would you actually do if someone used some embarrassing personal secret about you for blackmail? Think about this if, for instance, you are just about to send your CV in response to a job advertisement. Are you *certain* the recipient is honest? Social engineers have been known to publish bogus vacancy notices.

CONTROL OBJECTIVE: TO DETER, AVOID, OR PREVENT SOCIAL ENGINEERING ATTACKS FROM EVER OCCURRING

CONTROLS AGAINST SOCIAL ENGINEERING

There are many ways to categorize or classify information security controls, for instance technical versus nontechnical controls, or controls against the threats, vulnerabilities, and impacts. In the case of social engineering, I find it more useful to examine controls according to the stages of an incident where they primarily come into effect, that is pre-incident, para-incident (immediately before, during, or just after an incident) and post-incident.

Please note that I am focusing on those information security controls that are particularly relevant to social engineering *per se*. If a social engineer succeeds in breaching or bypassing these controls or if they are missing allowing an incident to occur, the eventual outcome will be determined by the presence and strength of many other information security controls such as user authentication and logical access controls, logging and alerting, and so on. Furthermore, the controls noted here are merely typical examples, not an exhaustive list, and may be insufficient for any given situation.

PRE-INCIDENT CONTROLS

The organization's information security policies, standards, and procedures should refer either directly or indirectly to social engineering, along with related topics such as fraud and hacking. They should be reasonably up-to-date, comprehensive, consistent, and usable (Peltier, 2001). They should be made widely available to current and new employees, for example through the corporate intranet. "Having a bunch of policies sitting in a red binder collecting dust atop an auditor's desk, is as useful as having no policies at all. I'll even argue that this makes an organization *less* secure, because it creates the illusion that steps are being taken to enhance security when nothing is actually being done" (Contos, 2006, p. 60. Emphasis in original).

Employee alertness is an absolutely vital control against social engineering, making this one of *the* most important security awareness topics. "Employees, contractors, and any other insider need to be educated on how to protect corporate assets. They need to understand the dangers and methods of social engineering and be careful what information they give out" (Cole & Ring, 2006, p. 41). Social engineers are highly sensitive to the reactions of their targets, so even the slightest hint of doubt or concern in someone's voice may indicate that their cover is blown. "Over the years and after doing several security assessments using social engineering techniques, nine times out of 10 we usually get caught when that one person says 'I need to call someone about what you're doing.' That call to confirm, usually raises enough suspicion to stop us from proceeding. And after that person realizes what they did, word travels real fast throughout the organization that they caught the 'bad guy'" (Stasiukonis, 2006). Unfortunately, social engineers tend to be very persistent too, so employees need to be quite assertive to resist social engineering attacks, assuming they recognize the signs in the first place. Awareness information and advice put employees in a much stronger position, helping them identify and deal with social engineers without upsetting genuine business contacts. The techniques to counter social engineering can also be learned and practiced. Best of all, "Security-awareness programs have the highest payback compared to almost all other countermeasures" (Winkler, 2005).

All "front-line" employees who routinely deal with visitors and callers (e.g., receptionists, Personal Assistants/secretaries, telephone operators, security guards, Help Desk, and call center staff) should be given specific training about how to recognize and deal with people who may be social engineers. "Guards should look closely at access badges. They should also search unusual packages and bags. They should patrol facilities, looking for things that are out of place. They should notice people in the buildings at odd hours, and they should question them and ascertain whether they are in the 'right' areas" (Winkler, 1997, p. 302). "Telephone receptionists should undergo intensive training so they can quickly recognize when someone is trying to pry information out of them" (Mitnick & Simon, 2005, p. 110). There is inevitably a trade-off to be made between the need to identify and reject social engineers versus the need to assist genuine visitors and callers. Training is important because the social engineering threat is not widely understood. Furthermore, because social engineers are encountered much less frequently than the genuine callers/visitors, refresher training and/or routine awareness materials should be used in addition to an initial session to achieve and then maintain sufficient awareness.

Other employees should also be offered training/awareness on social engineering because anyone may be on the receiving end of an attack. Pragmatic advice such as referring unrecognized phone callers back to the receptionists should be widely circulated. Contact points for further information might include the information security manager and the IT Help Desk to whom all possible or actual social engineering and other information security attacks should be reported.

Warning signs and physical access controls should indicate clearly that unauthorized access to corporate facilities is forbidden, and more broadly should make it obvious that unauthorized people are not welcome on site. The visible presence of security guards at the main reception area is one of the most common deterrent controls. Security guards may usefully check the identity of people entering the building, including in busy periods (perhaps checking anyone they do not recognize). Random stop-searches of people on site or as they leave site may also have a deterrent effect if well publicized. All entrances should be secured to a similar degree, including front and rear entrances, fire exits, goods delivery areas, and so on.

Logical access controls on the networks and systems should make it difficult for employees (perhaps under instruction from a social engineer) to install executable software or to access sensitive data areas beyond their job requirements (i.e., role-based access control). Furthermore, antivirus controls will significantly reduce the risk of malware such as Trojan horse programs including keyboard loggers, viruses, and so on.

The controls to prevent dumpster diving are mostly self-evident but, for some reason, are not commonplace. Confidential waste bins should be locked and preferably secured to the office. Anyone claiming to be a confidential waste contractor should be authenticated before the bins are released into their care. At the least, procedures should insist that waste contractors are summoned by authorized Facilities, Office Services, or Security staff rather than turning up whenever they like, and they must bring an empty but branded bin to exchange for each full bin removed. The contents of ordinary office waste bins should preferably not be left unsecured outside the office but ideally should be placed in a secure holding area and only released to legitimate garbage collectors.

Testing the effectiveness of, and compliance with, the policies, standards, and controls that address social engineering is itself a preventive control because it is an opportunity to identify and strengthen weaknesses in the system of controls. The Information Security Manager may choose to do such tests personally and/or to liaise with Internal Audit to this end, perhaps using the controls checklist included in this month's NoticeBored deliverables. Either way, if "physical penetration testing" is planned, it is extremely important that senior management are aware and approve of the testing before it starts, although it may be worth limiting this knowledge to the CEO and/or IT Director. For the tests to be truly representative of real social engineering attacks, the director/s should be persuaded to keep the tests confidential and not to pre-warn their colleagues, managers, or staff.

PARA-INCIDENT CONTROLS

CONTROL OBJECTIVE: TO IDENTIFY AND CHARACTERIZE ACTUAL SOCIAL ENGINEERING ATTACKS IN PROGRESS AS SOON AND ACCURATELY AS POSSIBLE, AND RESPOND EFFICIENTLY AND EFFECTIVELY

Employee vigilance is perhaps the most important way of detecting social engineering attacks if (or rather when) they occur. The awareness and training activities noted earlier are therefore doubly important in terms of both preventing and detecting these attacks. Furthermore, there should be standard procedures for reporting information security incidents, typically channeled through the IT Help Desk, sometimes supplemented by a dedicated "whistleblowers' hotline" for confidential reporting of insider threats, frauds, and other ethical breaches by employees and, in some cases, by outsiders. Encouraging and rewarding employees who report social engineering incidents is probably more beneficial in the long run than chastising those who do not. "Rewarding people for doing the right thing sends the right signal to others in the organization, while shooting the messenger in the case of a whistleblower allegation sends the wrong signal. . . . Organizations must go to extreme lengths to protect a whistleblower's identity and safety (from retaliation)" (Ramamoorti & Olsen, 2007, p. 55).

Incident response procedures are important for minimizing the impact of all forms of information security breach, including social engineering attacks. The organization should have well-written procedures in place for responding to and managing social engineering or other information security incidents, for example, notification of information security manager, circulation of general alerts, investigation and forensic analysis, and so on. Are the procedures clear and well-known? In particular, are front-line staff familiar with, and actually using, the notification/escalation steps at least?

Corporate facilities, and sensitive areas (such as the boardroom, managers', and HR offices) in particular, should be inspected from time to time for unauthorized surveillance equipment (bugs, keyboard loggers, network sniffers, wireless access points, and so on). The extent and frequency of such inspections depends on the organization's assessment of the risks. If this work is performed under contract by third party specialists, background checks should be made to establish their competence and trustworthiness for this work (the risks of employing organizations comprised of former hackers should not be underestimated). Ideally, they should also be monitored by employees, partly to check that nothing is installed by them and partly so that employees increase their own level of competence.

The "Caller ID" (also known as CLI/Caller Line Identity) facility on modern phone systems gives limited assurance of callers' identities. Even the simple fact that calls from internal phones normally have a different ring tone to external calls may give away a social engineer masquerading as an employee. However, employees should be aware that this control is imperfect—there are techniques for withholding numbers and redirecting calls so that they appear to come from different numbers. Skilled phone hackers ("phreaks") may even be able to manipulate the telephone system.

"Honeytokens" are artificially created data items (such as false customer records with tell-tale e-mail addresses) used by some organizations to lure hackers, data thieves, fraudsters, and others into betraying their presence (Spitzner, 2003; The Honeynet

Project, 2004). This approach suggests a way of exposing social engineers by challenging their insider knowledge, for example asking them to confirm a false name of a person, system, project, and so on, as in "You want to speak to Laura on the Help Desk: would that be Laura Smith or Laura Jones?" A genuine caller is arguably likely to offer Laura's correct name or admit that they do not know her name, whereas a social engineer is perhaps more likely to pick one of the offered fictitious names just to press ahead. Experienced social engineers, however, are equally likely to have the skills to evade such obvious traps.

POST-INCIDENT CONTROLS

CONTROL OBJECTIVE: TO LIMIT THE DAMAGE CAUSED BY SOCIAL ENGINEERING INCIDENTS

The organization's contingency plans should cater for all sorts of information security incidents, including social engineering attacks. Well thought-out contingency management processes improve the organization's capabilities to respond more effectively and efficiently to incidents regardless of their cause or nature—in other words, what people do is contingent (depends on) the particular circumstances that unfold. Examples of the sorts of things worth including in contingency plans are the means to call out relevant people urgently (e.g., up to date contact details with a "cascade" or "round robin" process), template public relations announcements, and procedures for salvaging information or other assets (e.g., off-site backups and IT Disaster Recovery arrangements).

Internal physical access controls should limit the ability of social engineers who succeed in physically entering the site from wandering about at will. Employees should be routinely instructed and encouraged to challenge unrecognized visitors. Additional access controls are sensible for areas containing sensitive information assets.

"Organizations must communicate to employees acceptable standards of behavior through a well-crafted code of conduct that is endorsed by leadership and enforced when necessary. Organizations should also develop a track record of acting swiftly and decisively whenever wrongdoing comes to light" (Ramamoorti & Olsen, 2007, p. 54).

Legal Department should advise on the possibility of responding to the loss of proprietary, personal, or other sensitive information to a social engineer by legal means. For example, there are usually requirements for IT forensic evidence to support a prosecution and such evidence must be gathered and retained in a particular way to be admissible. Factors such as this may impact the policies, standards, procedures, and even training, awareness, and other controls (e.g., warning notices may be required by law if surveillance activities such as telephone or closed-circuit television [CCTV] recording are to be used).

It is technically possible for the organization to obtain insurance policies covering direct and/or consequential losses as the result of a social engineering attacks. However, it may not be economically worthwhile. Check the policy terms and conditions, policy excess, and so on as well as the premium. It is often worth exploring the insurance option if only to get free advice from the insurance companies about the controls they would recommend to minimize the risks.

Do not neglect the final stages of a sound incident management process, namely a review of the risks and controls in place and, where justified, implementation of control improvements in light of the experience gained. Valuable information value can be gleaned from "near-misses" as well as actual social engineering incidents, for example better estimates of the frequency and nature of social engineering threats and clues about the vulnerabilities of most concern.

SOCIAL ENGINEERING CONTROLS IN ISO/IEC 27002

Social engineering is not directly addressed by ISO/IEC 27002:2005 (the international standard Code of Practice for Information Security Management) although several sections are relevant:

- □ Section 8 "Human Resources Security" includes 8.2.2 "Information security awareness, education, and training." This is the primary control against social engineering. Pre-employment screening identified in section 8.1.2 can also help keep potential social engineers off the payroll, although organizations need to be equally vigilant for employees who become social engineering threats during the course of employment.
- □ Section 13 "Information Security Incident Management" offers advice on reporting and responding to security incidents. If an employee is alert enough to appreciate that they are dealing with a social engineer, they should know what to do next, for example, refer the caller or visitor to specially-trained "front line" staff. If social engineering attacks are just ignored rather than reported, the Information Security Manager and management colleagues will never know the true extent of the threat.
- □ The physical access controls described in section 9 "Physical and Environmental Security" reduce the risk of unauthorized people entering and roaming around the premises, with even greater emphasis on secure areas such as computer and telecoms rooms.
- □ The logical access controls in section 11 "Access Control" reduce the risk of anyone getting access to sensitive data and functions on the computer systems and networks by any means, including social engineering. In other words, there needs to be a balance between technical and non-technical controls.

CONCLUSION

If one takes a moment to reflect, almost everyone is capable of social engineering to some extent. Any parent would surely recognize the persuasive power and manipulative nature of even a pre-school child. Committed social engineers take their art to new levels, finding plenty of opportunities and techniques to exploit innocent, naïve, careless, and unaware people.

Although security awareness/training is probably the strongest form of control against social engineering, I have outlined a number of preventive, detective, and corrective controls that, taken together, reduce the risks. Being realistic, however, I accept that social engineering is an extremely difficult nut to crack by any means. "The problem of social engineering should be recognized as difficult to solve; there is no solid assurance that any controls will work well" (Marks, 2008).

DISCLAIMER

The controls identified in this paper are generic, do not necessarily apply to any given situation and may not be sufficient for your specific requirements. They reflect published standards such as ISO/IEC 27002 combined with the author's practical experience. You should take further advice and assess the risks in your own situation to determine the particular security controls that are appropriate to your organization.

REFERENCES

Cole, E., & Ring, S. (2006). Insider threat: Protecting the enterprise from sabotage, spying, and theft. Rockland, MA: Syngress.

Contos, B. T. (2006). Enemy at the water cooler: Real-life stories of insider threats and enterprise security management countermeasures. Rockland, MA: Syngress.

Hitchcock, J. A. (2006). *Net crimes & misdemeanors: Outmaneuvering Web spammers, stalkers, and con artists*. 2nd edition. Medford, NJ: Information Today Inc.

ISO/IEC 27002:2005. International standard—information security—security techniques—code of practice for information security management. Geneva, Switzerland: ISO/IEC

Lininger, R., & Vines, R. D. (2005). *Phishing: cutting the identity theft line.* Indianapolis, IN: Wiley.

Marks, N. D. (2008). Personal communication to the author by e-mail. January 6, 2008.

Microsoft (2006). How to protect insiders from social engineering threats. Received January 4, 2008 from http://www.microsoft.com/downloads/details.aspx?familyid=05033e55-aa96-4d49-8f57-c47664107938&displaylang=en

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Indianapolis, IN: Wiley.

Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders, and deceivers.* Indianapolis, IN: Wiley.

Mitnick, K. D. (2006). Quoted by Talyn Halkin in *The Jerusalem Post*, February 24. http//www.jpost.com/servlet/satellite?cid=1139395477381&pagename=Jpost%2FJPArticle%2FShowFull

Peltier, T. R. (2001). *Information security policies, procedures, and standards: Guidelines for effective information security management.* Boca Raton, FL: Auerbach.

Ramamoorti, S., & Olsen, W. (2007). Fraud: The human factor. *Financial Executive* (July/August), pp. 53–55.

Rossiter, J. (2007). Secrets of Shell and Rolls-Royce come under attack from China's spies." Received January 4, 2008 from http://business.timesonline.co.uk/tol/business/markets/china/article2988228.ece

Schneier, B. (2000). *Secrets & lies: Digital security in a networked world.* Indianapolis, IN: Wiley.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world.* New York: Copernicus Books.

Spitzner, L. (2003). *Honeypots: tracking hackers.* Boston, MA: Addison-Wesley.

Stasiukonis, S. (2006). Banking on security. Received January 4, 2008 from http://www.darkreading.com/document.asp?doc_id=111503

The Honeynet Project (2004). *Know your enemy: Learning about security threats*. 2nd edition. Boston, MA: Addison-Wesley.

Wikipedia (2008). Entry for social engineering (security). Received January 4, 2008 from http://en.wikipedia.org/wiki/Social_engineering_%28security%29

Winkler, I. (1997). *Corporate espionage: What it is, why it's happening in your company, what you must do about it.* Rocklin, CA: Prima.

Winkler, I (2005). *Spies among us: How to stop the spies, terrorists, hackers and criminals you don't even know you encounter every day*. Indianapolis, IN: Wiley.

Gary Hinson is an IT governance specialist with a twenty-year career in information security management, IT risk management, and IT audit. He has worked for large and small companies in a variety of industries and has been consulting since 2000 (www.isect.com). Gary is passionate about security awareness (www.NoticeBored.com) and the ISO/IEC 27000-series information security management standards (www.ISO27001security.com).