

Reconnaissance: Social Engineering for Profit

Solutions in this chapter:

- Narrowing Your Choices
 - Digging for the Information
 - Researching for Rewards
 - Making the Contacts
-
- ☑ Summary
 - ☑ Solutions Fast Track
 - ☑ Frequently Asked Questions

Introduction

In this chapter, we discuss specific differences between in-house and contract employees, along with how federal work differs from the private sector. Different skill sets and background information are discussed and contrasted, and the importance of the Federal Information Security Management Act (FISMA) is explained. For contractors, the size of the contracting company is analyzed and comparisons created.

Intelligence gathering must be performed in order to make informed decisions about which companies to pursue. Finding out about company history, hiring, and layoff trends, as well as awards received and/or negative publicity are important to creating an informed picture of the company. The acquisition and divestiture trends of a larger company are also important in determining business growth.

Personal contact with employees and human resource personnel of the target company is very important. Attending job fairs, internships, and outreach activities make human resource personnel aware of your interest, as well as your desire to gain a position. Performing research into the company's activities and affairs puts you in a better position to make career decisions. This research also pays big dividends with the interviewers themselves and hiring personnel down the road.

How to behave and present yourself when making important contacts is also covered. Becoming knowledgeable and comfortable with topics common to the desired job is important to convincing personnel that you are the right person for the job. Areas of concern in contractual work are also discussed.

Narrowing Your Choices

Okay, you have studied all of your different options for work and have decided on what you think you want to do. Now you need to be able to take your defined skill sets and decide a few choice areas where you want to be. Although you do not have the job yet, you need to be able to see yourself 3 to 5 years in the future and what you would like to be doing. The first big choice is whether to pursue an in-house position or try your luck as a contractor or consultant.

In-House

With the explosion in need of INFOSEC, there are opportunities in almost every sector or industry that may interest you. If you have worked in the oil and gas industry for years and love the environment, set your sights on a job there. Play to your strengths and advanced skills. If your specialty is wireless, look for a company

that may have multiple work locations, some in remote areas, where wireless connectivity is more important than in a traditional office environment. Voice over IP (VoIP) is another technology many companies are embracing to cut costs between geographically-diverse offices. If you have experience setting up and securing an Asterisk server, put those together.

Here you will find your targeted skill engineering jobs – it's a great place to go if you are just making the transition from straight IT into INFOSEC. Take your skills with being a DBA and go for a security engineer's job where you will analyze user rights for usage of least privilege (only the minimum rights allowed for the task), inherited rights and permissions, known insecure methods and invocations (like the gratuitous use of `xp_cmdshell` in MS SQL Server). Jobs like these are more stable, and your job from day to day will likely not change much. You shouldn't get too many surprises, and it gives you the chance to really focus on your passion. Every IT-focused task needs to have an INFOSEC counterpart that understands the security implications of that task; remember this is not a solution, but a process.

Systems administration is a discipline that has been around as long as there have been computers. With the proliferation of interconnected systems, not only does the need for classical sysadmin duties arise, such as making sure resources are available in a timely manner, but so does the need for ensuring the security of those resources. Sysadmins should be security conscious already, so the leap into INFOSEC for this job is not great. Make sure that user rights are appropriate for file servers, mail servers, web servers, and other shared resources. You need to know what the baseline services are for each properly setup server, so that any deviance from that will be noted and researched.

If you come from a network engineering background, be aware that many of the devices you are used to working with don't have the best track record for security. Many devices don't communicate over secure applications; most use telnet, ftp, and SNMP v1 for remote access. Understand that since these are usually perimeter devices along with the LAN infrastructure, a compromise of either one seriously degrades the INFOSEC posture of the network. Take the time to research devices you currently use, and figure out how to secure access to them and their configurations. Network security is often overlooked at the infrastructure level versus the perimeter security of firewalls and remote access devices such as VPNs.

When you look at a typical network, either enterprise or personal, desktop management may take a lower importance than the server and network resources. Anyone that has done any penetration testing or security assessment can tell you that if you can compromise the workstations at the end-user level, you can greatly

increase any exposure in the entire network. Patch management, user rights assignment, and making sure that desktop security roles such as local administration are properly locked down, go a long way to ensuring the security of the environment.

As far as the work environment for an in-house INFOSEC job, it varies little from other in-house jobs in stability. Assuming the company is viable and hasn't had any serious incidents, the job can be considered stable. Unless you work in supporting multiple locations or remote sites, your travel will be light. If normality and small changes are what you crave, then definitely look towards an in-house position.

If you decide to go towards the government route, use the same thought processes, and go for an agency that best fits your interests and skill sets. Federal government agencies are required to submit yearly reports for the Federal Information Security Management Act (FISMA) where they are graded on an A to F scale on INFOSEC abilities. You can find a copy of the 2004 scorecard shown in Figure 2.1 below, at <http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf>.

Figure 2.1 FISMA Scorecard for 2003 - 2004

FEDERAL COMPUTER SECURITY REPORT CARD					February 16, 2005	
GOVERNMENTWIDE GRADE 2004: D+						
	2004	2003		2004	2003	
AGENCY FOR INTERNATIONAL DEVELOPMENT*	A+	C-	DEPARTMENT OF STATE	D+	F	
DEPARTMENT OF TRANSPORTATION	A-	D+	DEPARTMENT OF TREASURY**	D+	D	
NUCLEAR REGULATORY COMMISSION	B+	A	DEPARTMENT OF DEFENSE**	D	D	
SOCIAL SECURITY ADMINISTRATION	B	B+	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D-	D-	
ENVIRONMENTAL PROTECTION AGENCY	B	C	SMALL BUSINESS ADMINISTRATION	D-	C-	
DEPARTMENT OF LABOR	B-	B	DEPARTMENT OF COMMERCE	F	C-	
DEPARTMENT OF JUSTICE	B-	F	DEPARTMENT OF VETERANS AFFAIRS**	F	C	
GENERAL SERVICES ADMINISTRATION	C+	D	DEPARTMENT OF AGRICULTURE	F	F	
NATIONAL SCIENCE FOUNDATION	C+	A-	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F	
DEPARTMENT OF THE INTERIOR	C+	F	DEPARTMENT OF ENERGY	F	F	
DEPARTMENT OF EDUCATION	C	C+	HOUSING AND URBAN DEVELOPMENT	F	F	
OFFICE OF PERSONNEL MANAGEMENT	C-	D-	DEPARTMENT OF HOMELAND SECURITY	F	F	

* - Inspector General did not submit an independent evaluation of the agency's security management program as required by the Federal Information Security Management Act of 2002
 ** - No independent evaluation from the Inspector General was submitted in 2003

Prepared by the Government Reform Committee, chaired by Tom Davis, based on reports required by the Federal Information Security Management Act of 2002.

By looking at this, it is fairly clear which agencies have been working on improving their INFOSEC capabilities and which ones have not. If you are looking for a place where you might be able to provide some positive influence into a newer program, look at the lower scores. If you are more interested in more defined leadership and a consistent vision, try the agencies with the higher scores. Please note that these are cumulative scores for an entire agency, which might house several different departments. It may be that Department 1 scored an A+ where Department 2 scored an F to create the C score for the entire agency.

Sell Your Skillz...

What is FISMA and Why Should I Care?

When FISMA was enacted in 2002, it was a clear signal to the Federal Government that Information Security was to be taken seriously. It required several things to happen for each agency and provided a framework for that agency to be judged against the requirements and guidelines set forward by the NIST. The full copy of FISMA can be found at <http://csrc.nist.gov/policies/FISMA-final.pdf>. FISMA replaced the Government Information Security Reform (GISRA), which was part of the 2001 National Defense Act that required agency-wide risk-based INFOSEC programs, but did not have mandatory INFOSEC standards.

Basically, FISMA requires each agency to have their information systems audited every year and checked against the NIST requirements. The agency then submits proof of these audits and checks, which is then compared with the Report Grading Element, found at <http://reform.house.gov/UploadedFiles/2004%20FISMA%20Report%20Grading%20Element.pdf>. Often the success or failure of an Chief Information Officer (CIO) is weighed heavily against his agency's FISMA score.

Being knowledgeable about FISMA is a huge plus when you want to work for a federal agency. Budgets are often tied to FISMA scores, and being able to support the types of activities that FISMA rates is a big goal when doing INFOSEC for the government. You may also be able to find more detailed information about each department's individual FISMA scores from the agency's web site.

Contractor

When you make the decision to go to work for a consulting-based company, or as a contractor, you should also choose the kind of organization with which you feel most comfortable. One of the harsh realities of contractor work is that if your contracts go away and your company cannot find other work for you, you are likely out of a job very quickly.

With the big companies (over 5,000 employees), you will likely have more stability and feel more secure in your position. Larger companies will have more open contracts at any one time and finding “coverage” is not as much of a challenge, as long as your skills are useable. Also, the primary growth method of large companies is acquiring other companies and their contracts.

Medium-sized companies (500 to 5,000 employees), may not offer as much stability as the larger companies, but they are better poised to offer newer business services on a faster timetable. A medium-sized company can usually provide quicker access to resources to develop a new service, like software code review or database security testing. Medium-sized companies will likely not spend as much money on acquisitions, but rather, invest in research and development for new technologies for additional business offerings.

Small companies (fewer than 500 employees), are all about speed and maneuverability. They may not have the huge cash reserves or large contract portfolio of the larger entities, but they can adapt much easier to changing trends. As a result, the risk is significantly higher when you work for one of these companies, but the potential for reward is also higher. These companies usually are willing to invest some time—and money—into radical approaches if the potential is there for a new business opportunity.

Institutions of higher education are probably the most stable places to work, along with government jobs. As long as the budget does not dramatically change, you will likely be able to start and retire there. The benefits offered are usually better than some of the smaller and medium-sized companies, as well. One issue with educational institutions is that they are much slower to adapt to new trends, as a whole. As always, there are exceptions, some universities have started sharing more information about controlling disruptive technologies, such as Peer-to-peer (P2P) and IRC Bot nets.

As a contractor, your work is defined by the contract itself. There are differences between the way commercial organizations and government departments work, so their contracts have different information. There are many facets of contracts, and trust me, unless you have a burning desire to become a contracting officer, you don't

want to know too much about them. One big difference between commercial and government contracts is the “limitation of liability,” where you define how much the contractor’s company has to pay to the client if things go wrong. You will find this in commercial contracts but not in government contracts. Any government contract can be voided by the government, and all money paid to the contractor refunded to the government. The main point of this is, violating contract terms is serious, so make sure what you do is totally in line with the contract terms.

The language may be different, but most contracts have what is called a “Statement of Work,” or SOW. The SOW outlines the specific tasks a contractor is to perform for the client under the “Period of Performance.” When the task is complete, the tasks from the SOW is what your work will be evaluated against. Make sure when you go through your tasks, they match up against the SOW.

The kind of contract is important, as well; there are Firm-Fixed Price (FFP) contracts and Time and Materials (T&M) contracts. FFP is just what it sounds like. During contract negotiation, a price is agreed upon by both sides and fixed into the contract. This can be a problem if the INFOSEC workers doing the job are not represented well in the contracting phase. You might end up with a contract requiring you to build a firewall and secure 10,000 nodes, but only giving you 60 hours to complete the task. Also, FFP contracts have the “overhead” or money for costs such as office supplies, travel, and so on, specified up front, so those costs have the potential to cause problems, as well. FFP contracts are avoided as much as possible by contracting companies. You will find more FFP contracts for short-term contracts, anywhere from a few weeks to a year. T&M contracts are usually used for long-term contracts that run over a year in length. T&M contracts allow you to have flexibility in the time required to complete the tasks for the SOW. Just about every high-dollar value government contract is T&M based. Most contractors prefer to work on a T&M contract because if a task runs long, you will get paid for it, where you might not with a FFP contract that runs long.

When you are working on a contract, is it possible that your company is not the only one on the contract. In fact, on large contracts, it is likely that it are not. It is common practice for one company to have a contract, but not have the resources to complete all tasks for that contract. In that case, there will be a prime contractor, the one who actually wins the contract, and multiple sub-contractors, the companies that do the tasks the prime contractor is not equipped to do.

In contract work, you find some of the more specialized INFOSEC disciplines. While you still have the IT to INFOSEC-focused jobs, such as the network security engineer and system security engineer, there are also jobs such as INFOSEC business

analyst and penetration tester. These specialized jobs require a broad knowledge of different IT disciplines with very developed knowledge of INFOSEC and testing procedures. Coming from a hacker background, you should have the experience from doing ground-level work on securing and bypassing these disciplines; use it to your advantage, and seek out jobs like this that play to your strengths.

As far as work environment, there are no certainties. You may be working solely on the customer's location, adhering to their policies, or you could be out at a contractor's office. You may be considered an expert in the field, or you may be treated as a second-class employee because you are not in-house. Stability in contract work may be more risky, and there is a higher possibility that you may be out of work if the contracts for which you are qualified become hard to find; however, you also get the move of a chance to move around to different jobs and work with different technologies than if you worked at the same location for 10 years.

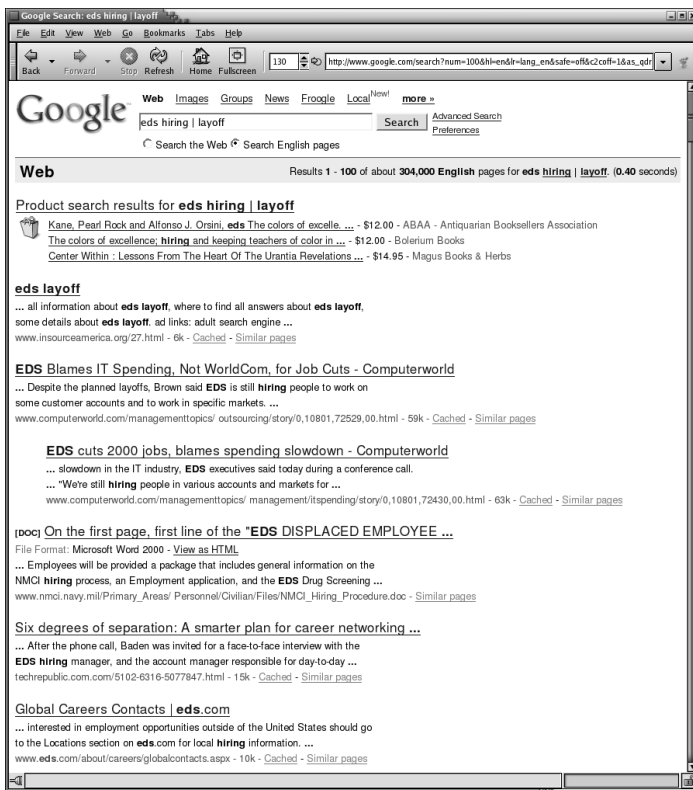
Digging for Information

Now that the targets have been identified, it is time to start working towards the new job you have always wanted. Like any successful hack, you have to know what you are looking for and the best place to find it. Company or institutional sites themselves often have tons of information that you can use to plan your approach to getting the job. News sites, from the global to the local, depending on the size of your target companies, are excellent places to start, as well.

Company History

The first thing you need to explore is if your target is actually hiring. Although the Careers or Employment section of that company's site is a great starting point, you should also check to see if there have been any events in recent history where that company went through a hiring frenzy or a period of layoffs. If they have positions for 30 INFOSEC engineers, but recently fired 100, you might want to look somewhere else. Figure 2.2 shows helpful information for using a Google search to find a job.

Figure 2.2 Google Search for Hiring and Layoff Information



From this example you can see that although the Careers page at EDS does show up, it also shows that EDS has also gone through a recent layoff cycle of at least 2,000 jobs. I crafted this Google query using the OR operator, represented by the pipe symbol (|). This is a basic example of an information search. For more advanced searches, we will use examples and information from Johnny Long's excellent book, "Google Hacking For Penetration Testers." Information like this is crucial for deciding which companies you want to move forward with.

Companies are often involved in the business of buying and selling other companies to gain additional expertise and/or contracts. Acquisitions and divestitures are common for larger companies. A smaller company recently acquired might be looking to replace or supplement existing staff. If you are interested in a particular company, check the state of the company's business growth. All of this information will be useful when building your resume and tailoring it for the company, as well as providing great "small talk" for interviews. The example in Figure 2.3 shows how to search for acquisitions and divestitures.

Figure 2.3 Google Search for Acquisitions and Divestitures



In this search, we look for information about Computer Sciences Corporation's (CSC) business activities buying or selling other companies. In the first six hits, we see references about three acquisitions and one divestiture, the divestiture being a company listed in the second hit, DynCorp. What we can learn from this is that CSC is actively participating in the business growth process and is likely to need more workers for new work gained from these acquisitions. Be wary, however, of a company that seems to do nothing but buy and sell smaller companies. They may not have a great strength in winning new work; their only work may be by what they can buy from smaller companies.

Good Results

A company that does well will often garner awards and recognition for their work. It is always a good idea to look and see if the company you are researching has

received any of these awards. There are some yearly awards that companies will often target, such as Forbes Magazine's "100 Best Companies to Work For." Access to the list requires a Forbes subscription, but they do allow you to search for free. If you receive a hit for your target company, you can follow up with another search for validation. Often CNN.com or money.cnn.com offer basic lists of these companies free, without registering. If you do a Google search for the "100 best places to work," you should be able to find the list for the last few years.

You can bet that if a company wins one of these awards, they will provide a link to that fact on their site. Make sure you do a detailed search of the Web site of your target for recognition. Many companies offer a Public Relations (PR) site that should summarize this information, or at least give you contact information to their PR people with whom you can follow up for more information. Again, information like this is great to use to customize your later efforts for a specific company.

Whether you are looking at a contracting job or in-house, new business coming in is crucial for a company's success. Has your target company has won new work recently? Many times a new win will directly correlate with hiring, especially in the contractor space. Since contracting and consulting companies often minimize overhead costs, they usually will not hire for potential work until the work is approved or granted.

Bad Results

Along with the desired qualities of your company, awards and recognition and new contracts, there are also times when companies get in trouble. As you are no doubt aware, anytime something bad happens in INFOSEC, there will be media there to convey the information. If a company is hit with items such as negative court decisions, governmental investigations into misconduct, or even grassroots protesting events, it can decrease the number of contracts or business awarded. In some cases, it may even result in layoffs or pay cuts.

For your desired company, make sure you check out the different news outlets, enforcement agencies, and international media outlets if your company does business out of the country. Being armed with information such as this will help you prepare for any "gotcha" questions later in the interview process. For example, if company XYZ was publicly chastised for a network intrusion that exposed the sensitive personal information of employees or clients, and you have experience in securing sensitive data on publicly-available systems, that is definitely something you should emphasize in your hiring process.

Seemingly “bad” things can have a positive affect on INFOSEC hiring. A company that has just gone through a high-profile compromise may bring on workers for a new approach to their security posture. A smaller company that might have had some problems and that had never understood the financial benefit in having INFOSEC might also decide to create a new capability and look for new personnel.

Researching for Rewards

Networking is an important aspect in finding that coveted INFOSEC job. You may feel that it is more important to know the field than to know who is in the field, and to a large extent, you are correct. However, it is much easier if you can leverage a personal contact when looking for employment. Many companies now require two to five references to be supplied when you apply for a job, and they will check them, especially when you are looking for security work.

You can hack away at a local target all day long and be very satisfied with the results, as well as make progress. Once you have learned all you can at that level, you need to start seeing how other remote resources affect your work. The same is true for job searching; you can base all your work on your own experience and knowledge, but take advantage, where you can, by making personal contact with those already working where you want to be. They are a source of information about a multitude of topics, including corporate culture, technical requirements, and contract information, as well as the all important, “How do you like your job?” Given this, you need to know some places where you can interact with these people in a relaxed setting to gain this valuable intelligence.

In the Front Door

Companies are interested in prospective employees who will take the time to search them out, rather than wait for a technical recruiter to track them down. Human Resource departments often host functions allowing job hunters to interact directly with those working in different areas of their company. Such functions are designed to give you access to these people in a professional setting and give you the chance to ask whatever you want.

Job Fairs

Whether they are hosted by your target company or by another organization, you should use job fairs to the fullest. They are free, usually common to larger cities, and draw lots of different companies. Do not go into a job fair thinking that you will be

walking out of there with a job, however. Companies will often perform “resume harvesting,” where they simply collect your resume in exchange for a pen or bag of marketing information. This is especially true in the larger fairs where 50-plus companies may be in attendance. Instead of using this opportunity solely to spread your resumes out, which you should still do, gain some person-to-person time with the recruiters and, hopefully, some of their INFOSEC employees.

Be direct with the personnel, and ask them questions such as, “Exactly what type of employees are you currently seeking?” “What types of skills are you requiring, and what skills would you prefer?” “Where will the work be located?” Something I have occasionally encountered are companies who attend job fairs with no jobs to offer. This is because some job fairs won’t ask companies to come back who do not buy a booth at every event. Therefore, in order for them to be able to represent their companies when they do need candidates, they attend and get resumes without any jobs to offer. Note that this is not an every time occurrence; most companies go to job fairs to find new candidates for jobs. Ask them if they are actually looking for new employees.

If you have several opportunities to choose from, try the ones hosted by the target company first, or try “Platinum | Gold | Silver” level sponsor. Also note that some companies have so many openings that they may offer multiple job fairs for different types of work. If you want to get more information about the cultural aspect of the company, attend those fairs to see if you can glean anything from the recruiters and attendees. Don’t limit yourself to strictly “tech” companies. At a multiple-industry job fair, ask a bank, grocery store, or chemical company about their IT department. The representative of the company may not be in charge of hiring for the IT department, but they may be able to put you in contact with the person who is. Job fairs also provide a great way to “practice” your interviewing skills and to get an idea of the types of questions that will be asked if you get an official interview. Use job fairs as R & D experience.

The Job Fair is the first place for you to sell yourself to a prospective company. You have a chance to talk with representatives in an open manner and ask questions that you may not want to ask in a more formal setting. You can make a good impression by asking targeted questions about a company’s particular need for INFOSEC, as well as give the impression that your skills will work towards their particular need. Making that first impression is critical, so make sure you present yourself in the most positive manner when you engage your prospective company at a job fair.

Internships

Internships are often the career path for those coming directly out of an educational track without much real-world experience. This is an excellent way to get knowledge about the company's operations and day-to-day affairs without being tied into them for a career. Although some internships do not pay, or do not pay well, they offer the advantage of making contacts in that company, and frequently lead to offers of employment.

It can be tough to get that first “real world” experience in INFOSEC, especially if you are still in school or don't have much other marketable experience. If you have the opportunity to qualify for some internships, you should try them out. Don't think that an internship forces you to work for that company; you may find out that the company you choose may not be the best place for you because of the internship. It is much better to find that out early, before you commit to work at place where you won't be happy. Even if you don't choose to go with that company for full-employment, you can still use that information on your resume. Many internships take place during summer breaks, especially those that have a multi-stage internship process. Some companies will have a first-level internship over a month during the summer, then pick their candidates to work the latter summer months, or even during a semester that you take away from your studies. Those often pay better, as you have to make up those hours you cannot take during that semester.

Outreach and Training Programs

Some companies practice outreach to the community by offering programs free of charge, or at a reduced rate, for topics like certification, personal skill development, or marketing. Seek out these programs as they are often taught or lead by skilled staffers volunteering their time for the company. This is a win/win situation. You gain personal contacts with the company; you learn something new, and you perceived as someone who takes personal time to better their skills and knowledge.

Look on the company's PR page or through press releases and you may find information about how a company sponsors a class or gives training for a particular topic. For example, Sentigy offers free-of-cost Certified Information Systems Security Professional (CISSP) training classes, taught by their employees. Other companies participate in similar programs to give their existing employees practice in presenting and teaching, while giving back to the community. If you have a particular topic that you want to get more information on, do some searches and see if your target company does anything like this.

Making Contact

Now that you have identified desirable options, it's time to gather more information about the company, as well as any functions you might attend to make personal contacts. It is time to move in and engage the target. When going through the initial meetings with the company, such as in job fairs or meetings, always present a good attitude. Read up on casual information about the company so that you are literate about their concerns in conversations. Be mindful of any constraints that they may require you to work under.

Improvise, Adapt, and Overcome

There are two keys to putting forth a good impression with HR personnel and company contacts. Blend in enough to not set off any alarms, but not so well that you are just another face in the crowd, and be flexible. You want to be able to present yourself as someone who can fit in with their company's culture without getting lost in the crowd. Also, flexibility is important, as sometimes a topic may come up that you haven't considered. Instead of reacting in surprise, take it in stride, and give some thought to it later, if it is an issue that will affect your decision.

Appearance and behavior will be discussed in later chapters, but to be brief, don't alarm anyone with your presence or activity. If you hope to sow anarchy and chaos wherever you go, professional INFOSEC is not the field for you, so save yourself some time now and look elsewhere. That being said, this is not "selling out." It is simply presenting yourself to prospective employers in the manner to which they are most accustomed. If you had wanted to never make waves and accepted anything presented to you, you would not be where you are with your skills. Employers want those skills, but they also do not want to be apprehensive about them. Putting forth a pleasing appearance is the first step.

Chances are, at a function such as a job fair, or a training program, you will not be hit with the most technical questions; those are reserved for interviews. Be prepared to speak in broad strokes, over high-level topics. If a topic is presented that totally throws you for a loop, say so, but be tactful about it. Suppose you are talking about alternative methods of authenticating users with an engineer and you're asked if you have ever used biometrics combined with PKI to authenticate a user. You may know how the two technologies are used separately, but have never touched on integrating the two. Be graceful and tell the interviewer, "I have worked with both of those base technologies and would be very interested to see how they work together in your implementation." If topics discussed cover an area where you have complete

mastery, let the person know, but again, be tactful about it. “Yes, I have three years of experience with that and am confident I could tackle any issue that comes up.” Keeping it high-level, discuss the foundations of your skills, including examples. All of these topics will be covered in more detail when we discuss the interview process in chapters to come.

Get the Background

Based on the industry or sector of your target company, become as knowledgeable as possible, if you are not already. Depending on the sector, there may be professional associations or affiliations that can provide background and detailed information about the sector. For example, if you are interested in a job within the energy industry, such as with an oil and gas producer, you can review the Security Guidelines posted by the American Petroleum Institute, at http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf. Also, being that this is a commercial entity, being familiar with ISO 17799 - Information technology - Code of Practice for Information Security Management would also be very useful. Although ISO 17799 requires a paid download, there are communities where it is discussed freely, so resources are available.

For those seeking a federal position, along with the previously mentioned FISMA, Certification and Accreditation (C&A) is currently a popular area for the entry-level INFOSEC candidate. Although there is much paperwork and manual process involved, C&A work includes technical and non-technical INFOSEC tasks, and is a good way to get a grasp on the complete Information Security Program concept. NIST has published SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Sell Your Skillz...

Get the Background

Any formal INFOSEC program is built on documentation, processes, and procedures. Those are heavily tied into those soft skills we discussed in the previous chapter. Although hard skills are required to get the job done, if you have some idea about the concerns of management, a more pleasant working environment will be assured.

Continued

Here are list of references you can use to become more knowledgeable with formal INFOSEC Programs.

- NIST Draft SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, <http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf>. HIPAA has become a huge force in the medical and insurance fields; many contracting companies are finding new business opportunities for INFOSEC in this field.
- NIST SP 800-64: Security Considerations in the Information System Development Life Cycle, <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>. Very dry information, but this is very important at the Security Program Manager level and higher.
- NIST SP 800-53: Recommended Security Controls for Federal Information Systems, <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>. Although this is not technically program-level information, it is a critical document to know when working in the federal space.
- NIST SP 800-30: Risk Management Guide for Information Technology Systems, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Understanding risk management will help you understand how vulnerabilities are rated and handled in a procedural manner.
- NIST SP 800-26: Security Self-Assessment Guide for Information Technology Systems, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>. Federal systems are required to perform a self-assessment yearly, as part of their reporting for FISMA. Many companies assist in compliance and audit base their activities off of 800-26.
- NIST SP 800-18: Guide for Developing Security Plans for Information Technology Systems, <http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF>. The System Security Plan (SSP) is the cornerstone document of any INFOSEC Program.
- Open Source Security Testing Methodology Manual (OSSTMM), www.isecom.org/osstmm/. Although this deals primarily with functional security testing, it covers in-depth procedures for the INFOSEC process.

Continued

- Sarbanes-Oxley (SOX) Act of 2002, www.aicpa.org/info/sarbanes_oxley_summary.htm. Like HIPAA, this law has forced some private sector companies into establishing a formal INFOSEC program.
- Financial Modernization Act of 1999, Gramm-Leach-Bliley Act or GLBA, www.ftc.gov/privacy/glbact/. Although financial institutions have historically been more current with INFOSEC than other industries, GLBA has required compliance.

Watch Out for Mines

Depending on the company you pursue, there may be unseen consequences and changes you need to make if employed. Employees of financial services corporations are often restricted from doing business with clients of the parent company, such as the use of credit cards, home loans, or stock ownership of those clients. If you work for a federal agency, there are strict rules that prohibit many types of gifts from vendors and other outside agencies. Many companies will ask you to sign a non-compete agreement stating you will not work for a company that does business with the same clients if you leave. In addition, Non-Disclosure Agreements are common today, so that any exposure you get to any sensitive technology or information is strictly governed. Consequently, when you make your first contacts, if you have strong feelings about these topics, it is best to get them answered quickly so you can adjust your pursuit.

Sell Your Skillz...

Fire for Effect

Here we walk you through a successful reconnaissance of your target, ABC Corporation.

First, look at the Site Map and find their Public Relations page, which states they received the MadeUp Magazine's Award for Top 50 IT Firms to Work for. Their PR page also states that they recently won a \$300 million contract to provide secure wired and wireless network deployments for XYZ Corporation. In doing a DejaNews search from <http://groups-beta.google.com/>, you find some messages from people with the

Continued

ABCcorp.com e-mail address asking questions about advanced Public Key Infrastructure (PKI) and secure wireless communications using Over The Air (OTA) re-keying.

Since the mid-sized company is located in Anytown, you check out the Anytown Courier newspaper Web site and discover that ABC has been working with a series of volunteers providing secure network access to local school districts and libraries. You go out and spend a weekend working with their engineers in wiring up the local library, making valuable contacts. You find out that these engineers really love their job; one of them has worked for ABC for 10 years. ABC is a large sponsor at a local job fair, so you attend the fair wearing business casual clothes (tie and slacks for men, comfortable blouse and either skirt or pants for women) with a stack of resumes. You meet the recruiter and two of the engineers you met at the volunteer weekend and discuss their recent business win, as well as your high-level of skill with both PKI and dynamic wireless re-keying. You learn they are starting to gain some work doing HIPAA and SOX compliance.

Now you know they will be looking for someone to do PKI and wireless, as well as be knowledgeable of HIPAA and SOX compliance auditing. This gives you an opportunity to study those topics and refresh your memory before you go in for an interview.

Checklist

- Are you comfortable in making the decision whether to work as a contractor or in-house?
- Do you know what types of information you need to discover about your target company?
- Do you know where you can go to have face-to-face interaction with company employees and get a feel for the job?
- Can you research and find out key topics that you may be questioned on during the interview process?
- Are you aware of any contractual issues that will affect the performance of your desired job?
- Can you discuss the regulatory issues your company may be compelled to follow?

Summary

Being able to determine which type of job you are seeking is crucial. In-house and contract employees have different challenges. If you decide to pursue a federal job, FISMA scores are a starting point, as well as a goal for understanding the environment.

Much information is available publicly for federal and private sector companies. Recent contract wins and any enforcement action should be noted, as well as awards and recognition for outstanding work and employee satisfaction. Purchases and sales of smaller companies are a good indicator of business growth opportunities, as well as knowledge about skills important to the company.

In order to gain internal information about the company, try to get personal interaction with employees of your target. Human Resources departments sometimes hold job fairs or community outreach allowing you to get more information about the employees and their opinions. Research into newsgroups and mailing lists can turn up topics of interest to the company. Knowledge of regulatory environments for the company's customers is critical for interview stages.

Solutions Fast Track

Narrowing Your Choices

- ☑ For in-house work, try to match up your skill sets to a company with the same needs and challenges, in other words, remote connectivity, database intensive operations. Federal work needs to correlate to FISMA requirements.
- ☑ Contractor work varies, but is still skill oriented. Large companies have stability, but are slower to move. Medium-sized companies are less stable, but more likely to create new opportunities. Small companies have a high level of risk, but are very flexible for new business and if successful, they are likely to be acquired.

Digging for Information

- ☑ Search for company history on hiring and layoff trends.
- ☑ Search for acquisitions and divestitures of smaller companies to find out growth potential.

- ☑ Determine if your target company has received awards for work or satisfaction, or has been involved with recent business wins. Make sure your prospect does not show up as having excessive compliance issues or enforcement actions.

Researching for Rewards

- ☑ Use Public Relations and Human Resource departments to gain personal interaction with employees.
- ☑ Job fairs and outreach programs are a good way to gain face time with the target company.
- ☑ Internships are a great way in for candidates recently out of educational work.

Making the Contacts

- ☑ Blend in for personal interaction, and be flexible with your responses.
- ☑ Try to keep talking at a higher level; don't overload the person with all your skills.
- ☑ Find out background information, such as compliance or regulatory environments.
- ☑ Be aware of contractual issues within a particular job or industry.

Links to Sites

- <http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf>. Most recent FISMA scorecard..
- <http://csrc.nist.gov/policies/FISMA-final.pdf>.
- <http://reform.house.gov/UploadedFiles/2004%20FISMA%20Report%20Grading%20Element.pdf>. FISMA Grading Elements.
- http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf. American Petroleum Institute Security Guidelines.

- <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>. NIST SP 800-64: Security Considerations in the Information System Development Life Cycle.
- <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>. NIST SP 800-53: Recommended Security Controls for Federal Information Systems.
- <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. NIST SP 800-30: Risk Management Guide for Information Technology Systems.
- <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>. NIST SP 800-26: Security Self-Assessment Guide for Information Technology Systems.
- <http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.pdf>. NIST SP 800-18: Guide for Developing Security Plans for Information Technology Systems.
- www.isecom.org/osstmm/. Open Source Security Testing Methodology Manual (OSSTMM).
- www.aicpa.org/info/sarbanes_oxley_summary.htm. Sarbanes-Oxley (SOX) Act of 2002.
- www.ftc.gov/privacy/glbact/ Financial Modernization Act of 1999, Gramm-Leach-Bliley Act or GLBA. X<http://groups-beta.google.com/> Google interface to DejaNews.

Mailing Lists

- www.fortune.com/fortune/technology/articles/0,15114,1024072,00.html. Did bring up a lot of popups though. Fortune Magazine's 100 Best Companies to Work for: requires subscription, but is searchable.
- www.computerworld.com/careertopics/careers/report/. Computer World 100 Best Places to Work in IT in 2004.
- http://expertanswercenter.techtarget.com/eac/knowledgebaseCategory/0,295197,sid63_tax296929_idx0_off50,00.html. Infosec Careers information in a question/answer format.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to www.syngress.com/solutions and click on the “Ask the Author” form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: When you talk about in-house work being stable, does that mean boring?

A: Not at all, in-house work is more stable from a skill perspective. The systems are less likely to change, and you will be working in a more stable environment than a contractor would. Those for whom constant change is stressful would usually be happier with in-house work.

Q: Why are you pushing so much information about federal systems?

A: The federal government has been hiring much more INFOSEC since the attacks of September 11, 2001. With the enacting of the FISMA legislation, many agencies were behind on the formal INFOSEC process and still need lots of support to become compliant. This has caused the Washington DC Metro area to become a very popular place for employment.

Q: You keep referring to the NIST Special Publications; why is that?

A: Commercial space doesn't have the same regulatory requirements as in federal work. Therefore, there is little base documentation. Much research and testing has gone into NIST documents, and they are a fantastic free resource for INFOSEC professionals.

Q: I don't see the value in understanding why ABC Company has been buying and selling smaller companies recently.

A: When all is reduced to the bottom line, companies survive to make money. Understanding how they spend their money on new companies to buy new work and processes is important to you so you will have new chances to work. If

a company is selling off assets, such as companies, without winning new business, they are less likely to grow and need new workers.

Q: Do you really think spending a weekend volunteering to gain some kind of personal interaction with different company employees is going to help?

A: Yes. When different candidates are being considered for the same job, especially for entry-level positions, it can be the smallest difference that may influence the decision. Being known to the hiring personnel or workers as someone who takes the time to help out and learn new skills is a big plus in your favor.