Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Practical Application of Background Investigations for Small Company Security Perimeters

e suffered losses due to insider threats and 7 percent of respondents thought that insiders account for more than 80 percent of their organization s cyber losses....

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

A Practical Application of Background Investigations for Small Company Security Perimeters

GSEC Gold Certification

Author: Timothy C.B. Cook

Adviser: Jim Purcell

Accepted: June 15, 2007

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Abstract

Companies spend millions of dollars every year to implement applications and hardware for the sole purpose of preventing outside entities from exploiting their computer resources, yet each year it is reported that the majority of Computer Security Incidents involve unauthorized access by insiders. Many of these incidents might be avoided if some form of background investigation were conducted on employees prior to providing them with systems access privileges or elevating their level of access. The moment someone suggests "Background Investigations" it brings to mind Department of Defense Security Clearances and Defense Security Service Personnel (in black suits and sunglasses, of course) interviewing friends, family and coworkers to determine if the individual is a "Risk to National Security," however background investigations need not be that invasive nor that expensive. The extent of the background investigation should be determined by each company, as a component of their Security Perimeter, based on the sensitivity of their systems and the extent of their budget and can cover the spectrum from none to extensive. In this paper I will suggest several means that companies can utilize to improve their security perimeter by performing simple background investigations at a minimal expense.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Abstract **2**

Acronyms **4**

Disclaimer **5**

Introduction **5**

Government Background Investigations **7**

So How Does This Relate To Non-Government Employment? **8**

First, Some Necessary Groundwork **9**

Who Should Be Investigated? 10

Fair Credit Reporting Act (FCRA) 12

Freedom of Information Act (FOIA) 14

Privacy Law Of 1974 15

Waiver 16

Gathering the Information **17**

Addresses and Phone Numbers 18

Education 20

Work History 21

Employer and Character References 23

Social Security Number (SSN) 24

Credit Reports 26

Criminal Records 27

What Information should you trust **30**

Summary **31**

References **33**

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Acronyms

BI	Background Investigation
CRA	Consumer Reporting Agency
CSI	Computer Security Institute
DiD	Defense in Depth
DOB	Date of Birth
DOD	Department Of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
NCF	National Criminal File
NCIC	National Criminal Information Center
OPM	Office of Personnel Management
PR	Periodic Reinvestigation
PSI	Personnel Security Investigation
SSA	Social Security Administration
SSN	Social Security Number
VPN	Virtual Private Network

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Disclaimer

I highly recommend that you consult legal consul before gathering any information on anybody (whether in your employ or not). While it is not my intent to provide information that contributes in any manner to any illegal activity and while, to the best of my knowledge, none of the actions or procedures that I describe here in violates any state or federal laws, I *have* been wrong before (ask my wife).

In addition, I make no claims or assertions that anything discussed in this paper is legal in the State of California. Nor will I assume that it is not known to the State of California that the mere reading of this document, in either electronic or reprinted format, may cause cancer in laboratory rats.

Introduction

According to the 2003 CSI/FBI Computer Crime and Security Survey, the two most cited forms of computer attack or abuse were "virus incidents (82 percent) and insider abuse of network access (80 percent)" and according to the 2005 CSI/FBI Computer Crime and Security Survey "despite some variation from year to year, inside jobs occur about as often as outside jobs." This data is confirmed and supplemented by the 2006 CSI/FBI Computer Crime and Security Survey where it is reported that 62% of respondents believe that they have suffered losses due to insider threats and "7 percent of respondents thought that insiders account for more than 80 percent of their organization's cyber losses."

Further, though you may completely trust all of your employees,

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

if you outsource any of your computer work, the damage need not come from "your" employees. According to the 2006 CSI/FBI report 39% of all Computer Security functions are outsourced. As stated by William T. Tucek (2003) "The biggest potential for risk and an innate factor with outsourcing, is the act of giving a third party, the outsource vendor, access to your organizations information. This information can include confidential information such as financial, medical information, records and strategic development. Along with the access, is the possibility of unwanted disclosure, alteration or destruction of the information. The possible impact here to the organization is loss of reputation, competitive edge and legal risks."

To look at this from the other side of the "outsourcing fence," if your company provides services to another company (consulting, application development, data storage or support in any manner) then you should be aware of the potential for negligent hiring lawsuits.

> Under a negligent hiring cause of action, an employer may be liable where a person is harmed by one of its employees, the employer knew or should have known through a reasonable investigation prior to hiring that the employee was unfit, and injury to the third party was proximately caused by the employee. In laymen's terms, this means that at the time of hiring, the employer knew or should have known that the employee who later harmed the third party was unfit for employment (Riley, 2003).

To simplify this even further, your worries can extend beyond what damage your employees may inflict on you to what they may do while they have access to a customer's facilities or resources.

Defense in Depth (DiD) is an approach to Information Security that relies on applying an appropriate combination of Physical, Technical and Administrative controls at strategic points of the Information Systems environment in order to create a security

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

perimeter that effectively addresses each risk in the most cost effective manner. The information cited above clearly illustrates the need for a Defense in Depth that includes administrative controls applied to your company's personnel. One such administrative control that is easy to apply and can be relatively inexpensive to employ is a Background Investigation (BI). While a larger company may choose to contract BI services from an external entity, often a small company may not feel that they have the resources to commit to this solution. However a BI need not be overly complex or resource intensive and can be easily conducted internally. Ultimately, a working knowledge of the methods employed in, and the restrictions on, a BI can be a valuable addition to your Security Tool Box - even if your company does make the decision to purchase BI services from an external entity.

Government Background Investigations

Though most people think about the U.S. Military when they talk about Government Security Clearances, the military is not the only governmental body that issues clearances.

> Security clearances can be issued by many United States government agencies, including the Department of Defense, the Department of Energy, the Department of Justice, and the Central Intelligence Agency. Department of Energy clearances include the "Q","R" and "L" levels. Most security clearances are issued by the Department of Defense and include Confidential, Secret and Top Secret (Dice, 2006).

Regardless of the issuing organization though, YOU can't request a security clearance. The request must originate with a Security Officer or other authorized employer representative. In addition, you will only be granted a security clearance that is commensurate with your job requirements and you will most likely be required to submit to a personnel security investigation (PSI).

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

A PSI is essentially a background check, but it's likely to probe deeper than a typical, employment-related check. It consists of one or more of the following, depending on the type of security clearance.

- Verification of U.S. citizenship
- Search for investigative files and other records at Federal agencies, such as the Federal Bureau of Investigation (FBI)
- Search for criminal records at local law enforcement agencies
- Fingerprinting
- Polygraph exam (lie detector test)
- Credit and other financial checks
- Check of records at courts, rental agencies and your employers
- Interviewing your references
- Interviewing you (Niznik, 2003)

The scope of the investigation will vary depending on the security clearance required and is designed to determine if the individual meets certain criteria "relating to their honesty, character, integrity, judgment, mental health, and association with undesirable persons or foreign nationals" (Federal Bureau of Investigation, n.d.). To this end you are requested to sign a form "authorizing release of ANY information about you to Security Clearance Investigators. This means that investigators can access any and all information about you, including sealed records, juvenile records, expunged records and medical records" (Powers, 2007a). Failure to provide this authorization is sufficient cause to deny you a security clearance. As of February 2005 all PSIs for government security clearances are conducted by the Office of Personnel Management (OPM) and can cost in excess of $10,000 (Hurley, 2005).

So How Does This Relate To Non-Government Employment?

OK, so now that we know a little bit about the personnel

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

security investigation conducted by the Office of Personnel Management while validating requests for government security clearance, you may be wondering "how does this relate to a small company performing its own background investigation?"

I'm glad you asked! As is true with most citizens of most countries, I can point to one or two things that our government does not do well. However background investigations are not among them. They may take a long time and cost a lot of money, but they are done very well. In fact, I would, and will, go as far as to say that the U.S. government sets the standard for background investigations. So rather than re-invent the wheel, we should attempt to utilize the PSI as an example for our own background investigations. Of particular note is how the OPM not only validates information that individuals have provided and examines information that is available through records, but also how they utilize the information that they gather. Remember, the ultimate purpose of a PSI is to determine if the individual can be trusted with the access being requested.

First, Some Necessary Groundwork

Before we go any further I would like to discuss a couple of important issues. Namely the issues of on whom you should gather information, when you should gather it and what information you do and do not have a right to gather. Three Legal Acts that are of particular importance to the collection and use of information about individuals are the Fair Credit Reporting Act (FCRA), the Freedom of Information Act (FOIA) and the Privacy Act of 1974. Together these determine what is considered "public" information and how this information may be used. As I am not an attorney (nor do I play one on TV) whenever possible I have utilized quotes from individuals or sources that are qualified to interpret or explain the intricacies or implications of these documents. In addition to the above mentioned

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Legal Acts most states also have laws that further define and/or restrict your rights to access an individual's public records. As I stated earlier "I highly recommend that you consult legal consul before gathering any information on anybody (whether in your employ or not)." I know that this may not be very exciting reading for some but I have included this information because, rather than just tell you "don't do that", I wanted to try to provide a little bit of information on why you shouldn't "do that."

Who Should Be Investigated?

While some individuals will state that the answer to this question depends on who you trust, I think that a better approach is to determine what resources you are trying to protect. Once you have determined *what* you are trying to protect, you can proceed to determine from *whom* you are trying to protect it. As that list can conceivably be quite long, a more practical method might be to develop a "short-list" of individuals in your company (or outside of your company perhaps) who need to have access to these resources or whose job responsibilities bring them into proximity with these resources. It is best to keep this list as short as possible. Develop the list and then reexamine each individual or position again. Do they really need that access? Are you justified and within your legal rights to investigate the individual? As will be explained in more depth later, some information is not legal to use in evaluating a person for employment.

Inherent to this approach is the concept of "trust nobody" (I know that sounds paranoid, but I have always believed that two noids are better than one). Honestly, until you have investigated an individual, how do you know that they are who (or what) you think they are? After all, one of the things that most serial killers have in common is that after they are caught somebody is quoted as saying

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

"he was such a nice man...who would have thought that he was capable of such a thing?"

Of course there may be times when the "trust nobody" mantra is not practical to apply. One such situation might be when working with staffing or consulting firms. Should you trust that an external staffing or consulting firm has performed their due diligence in investigating their employees, or should you insist on seeing documentation, proof of certifications and background checks? Personally, I don't think that you should accept somebody else's word on their employees' background; demand proof! While the potential for penalties may cause agencies and people to be careful, what good is suing an external entity after the damage is done? Does it clear your company's reputation or bring back your lost business?

At the end of the day, what use is a Company's investment in VPNs, encryption, firewalls, security guards, etc. if they proceed to hand the keys to their kingdom to the bad guy? As we stated earlier, the biggest potential for risk a company can have is the act of giving an individual access to company resources, either physical or electronic. Ultimately it is your responsibility to protect yourself.

Just as important as *who* should be investigated is *when* they should be investigated. The ideal rule to follow, of course, is to be "Pre-Active not Re-Active." Remember, the situation that you are addressing is not one of "close the doors before the horses get out," but rather "close the doors before the mountain lion gets in." In other words, in this particular scenario, you are not concerned with what dangers lay outside your barn but rather what dangers you are allowing into your barn. Hopefully all of this emphasizes the point that the best time to investigate an individual is before you hire them and/or elevate their access to your company resources, not after. While that was very easy for me to type, I realize that it is

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

not always easy to implement.

Additionally, just because an initial background investigation has revealed no obvious cause to distrust an individual, do not assume that this will always be the case (refer to my earlier comment concerning "noids"). It is entirely possible that either something of concern was not initially reported/discovered or that something of relevance has occurred since the initial investigation. Because of this, background investigations should be reviewed and/or re-conducted both periodically and prior to the escalation of any access to resources or increase in responsibilities. The policy utilized by the U.S. Federal Government in regard to security clearances, is that "a Periodic Reinvestigation (PR) is required every 5 years for a TOP SECRET Clearance, 10 years for a SECRET Clearance, or 15 years for a CONFIDENTIAL Clearance. However, civilian and military personnel of DOD can be randomly reinvestigated before they are due for a PR" (Powers, 2007b). Finally, when creating any policy regarding security, be sure to evaluate it against your company's security policies to ensure that your posture aligns with that of your company.

Fair Credit Reporting Act (FCRA)

Now that we have some ideas of "who" and "when," we need to look at some of the restrictions concerning "what." The Fair Credit Reporting Act (FCRA) is a good starting point for this topic. The following excerpt from CreditReporting.com "Fair Credit Reporting Questions and Answers" page is probably the best introduction to the FCRA that I have encountered during my research for this paper:

> If you've ever applied for a charge account, a personal loan, insurance, or a job, there's a file about you. This file contains information on where you work and live, how you pay your bills, and whether you've been sued or filed

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

for bankruptcy.

Companies that gather and sell this information are called Consumer Reporting Agencies (CRAs). The most common type of CRA is the credit bureau. The information CRAs sell about you to creditors, employers, insurers, and other businesses is called a consumer report.

The Fair Credit Reporting Act (FCRA), enforced by the Federal Trade Commission, is designed to promote accuracy and ensure the privacy of the information used in consumer reports. Recent amendments to the Act expand your rights and place additional requirements on CRAs. Businesses that supply information about you to CRAs and those that use consumer reports also have new responsibilities under the law (Creditreporting.com, 2007a).

Now that we know something about what the FCRA is I will list some matters concerning the FCRA and CRAs that are of particular import to this paper:

1. "The employer must obtain the applicants written authorization before the background check is conducted. The authorization must be on a document separate from all other documents such as an employment application" (Privacy rights clearinghouse, 2007).

2. CRAs are forbidden from providing information that it has gathered to entities that can not prove a legitimate need or do not have written consent from the subject of the report.

3. There is no guarantee that the information in the consumer report is correct.

4. If an individual is denied employment based on the content of the consumer report they must be provided with the name, address and phone number of the CRA that provided the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

consumer report (Creditreporting.com, 2007b). In addition they must be provided with a notice that the potential employer made the decision to deny employment, not the screening company, as well as a notice that the individual has a right to dispute the accuracy or completeness of any information with in the consumer report.

5. If a CRA, a user, or a provider of CRA data violates the FCRA, they may be sued in state or federal court (Creditreporting.com, 2007b).

The full text of the Fair Credit Reporting Act (15 U.S.C. §§1681-1681u) is available from the Federal Trade Commission (FTC) at http://www.ftc.gov/os/statutes/fcra.htm.

Freedom of Information Act (FOIA)

The FOIA, as it applies to this paper, concerns the rights of the public to access information gathered by the U.S. Government. It was signed into law by President L. B. Johnson in 1966 and "generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions (United States Department of Justice, 2004)." The most pertinent (to this paper) of these exemptions are number 6, which protects an individual's personnel and medical files, and number 7 which protects:

> Records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

> constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual (Wikipedia, 2007).

The full text of the Freedom of Information Act (5 USC §552 (1966)) can be accessed from the United States Department of Justice (DOJ) web site at http://www.usdoj.gov/oip/foiastat.htm.

Privacy Law Of 1974

According to the Electronic Privacy Information Center (2003)

> The Privacy Act of 1974, Public Law 93-579, was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it lets individuals sue the government for violating its provisions.

The disclosure rules are listed in subsection (b) of the Act and are preceded by the statement "No agency shall disclose any record which is contained in a system of records by any means of

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." One of the following allowable disclosures of personally identifiable information that is pertinent to this is "to a consumer reporting agency in accordance with section 3711(e) of Title 31." The full text of the Privacy Act of 1974 (5 USC §552a) can be accessed from the United States DOJ web site at http://www.usdoj.gov/oip/privstat.htm.

Waiver

From dictionary.com:

Waiv-er (wey-ver) -noun Law

1. An intentional relinquishment of some right, interest, or the like.
2. An express or written statement of such relinquishment.

One of the defined allowable disclosure criteria, as quoted above, was "except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." One manner to acquire this written permission is to have your employee, or potential employee, read and sign a waiver form. You can get an attorney to create a waiver for you or you can download a generic waiver from the internet, the choice is yours. Generally speaking a waiver should exist on a document separate from all other documents and should clearly inform the individual what information you intend to access as well as how it will be utilized. A key aspect of waivers is that the individual must understand what right or rights they are waiving. For this reason it is recommended that the waiver be specific about what information is going to be collected, how it is going to be collected and for what purpose it is going to be collected.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Gathering the Information

As we saw above, information about individuals is collected by both governmental and public agencies and there are federal and local laws governing what can be gathered, what should be disclosed and what should not be disclosed. Something that you also need to consider is that just because a waiver may make information available to you doesn't mean that you have a right, or a need, to see the information! As we often caution superusers - "Just because you can do something doesn't mean you should."

As I discussed in the "Who Should Be Investigated" section, your primary purpose in conducting an investigation is to determine whether you believe that the individual can be trusted with your Company's resources. A good place to start your investigation is by attempting to verify that the information that the individual has already provided you is complete and correct (after that you can start searching the internet and other public records). Typically this information will be provided to you by the individual in the form of a resume and/or a completed Job Application form. The Job Application form usually requests such information as the individual's full name, current and past addresses, phone number, Social Security Number (SSN), references, previous employers (including job titles and dates of employment), education and to list any felony convictions. The more information you can have the individual provide you the better, however here you must be careful as well because

> State and federal laws protect job applicants and employees against various forms of discrimination. At the federal level, there are prohibitions on employment discrimination based on race, color, religion, sex, national origin, pregnancy, age, citizenship status, disability, military status, and union membership. State and local laws can be even more inclusive, protecting characteristics such as

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

> sexual orientation, marital status, and even smoking habits. If application forms or interviewers ask questions that are not clearly job-related, or that tend to reveal an applicant's membership in any of these protected classes, you are risking a potential discrimination claim (Personnel Policy Service Inc., 2007).

After the individual is in your employ different rules apply and it may be permissible to require an employee to complete a Security Investigation Questionnaire (after signing a waiver, of course) before systems access is granted, though I would still clear everything with your company's legal consul first. Also, a word of caution: Think twice about performing internet searches that include confidential information as there is the potential that your queries could become publicly available (as occurred with AOL in August 2006)!

Addresses and Phone Numbers

An internet search for "online phone book" or "online yellow pages" will quickly yield multiple sites that you can be used to verify phone numbers and addresses. One such site is http://people.yahoo.com which allows you to look up individuals utilizing their first and last name as well as either a state or a city and state. One advantage to a city-less search is that while you may know that an individual worked for a company located in a given city, that does not mean that the person lived *in* that city. Unless the individual has a very unique name it is likely that an online phone book search will yield multiple hits - hopefully containing the individual's current address and phone, possibly containing the individual's previous addresses and phone numbers and most likely containing information on other individuals in that area who share the individuals name and are irrelevant to your investigation. Also, only a click away from this Yahoo site is the Intelius search engine (http://find.intelius.com/people-search.html) that can be utilized to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

perform a simple and free "people search" that will list known cities of residence as well as, at times, an individual's age and known relatives. While you may or may not care about the relatives, depending on the information that you are validating, the age could be useful in confirming that the information that your search returns is for the proper individual.

Another method to possibly confirm a phone number and address is to visit a site, such as http://www.daplus.us/PhoneSearch.aspx, that will allow you to perform a reverse phone search in which you enter the phone number and search their database for any names and addresses associated with that number. While this is actually quicker than a forward search due to the fact that you don't have to sift through the "others" with the same name, it requires that you have a phone number for each name/address that you wish to confirm. Another consideration is that if the individual is still living at home (or any place else where the utilities are not in their name) then this may be a better method to confirm their phone number and address as it may match the phone number and address as well as provide the name that the phone is registered to.

Alternately there is the low-tech approach. Unknown to some, way back "in the day," before everybody had home networks and internet in the living room, there were only two ways to look up a phone number. Either you could acquire a "White Pages" phone book for a given city (often larger than an encyclopedia) in which you would attempt to locate the persons name alphabetically (provided that the page you need hasn't been torn out) and then search amongst the names for the associated address, or you could call "Directory Assistance" at the easily remembered phone number of 1-800-555-1212 (or <area code> - 555-1212 or just 555-1212 if dialed within the associated area code). Before long a helpful person will answer and ask the name and address of the individual whose number you would like them to locate. I must

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

admit that I had to call the number just to see if this service was still available.

Another possible route is to utilize online mapping and satellite image services. Google Maps (http://maps.google.com) is particularly useful for this as you can search for a business and map it simultaneously. Once you have a residence, employer or university's location verified through the mapping services you can go one step further by evaluating the satellite image of the address to see if the buildings look appropriate for the occupant. For example, if the address is supposed to belong to a physical university then the satellite image should show several (or many) large structures and if it is supposed to be a residence then it most likely shouldn't be in a large office complex.

If you succeed in confirming the individuals address and phone number then "good for you." However if you do not succeed it does not necessarily mean anything. Among other things, if the individual has recently acquired a new phone service, chosen to have their contact information "unlisted" or "unpublished" or even listed under another persons name then the search will probably not be successful. This is not a big deal though as this is not a "Pass/Fail" sort of check, but rather a "confirmation of information provided" check.

Education

I know this will come as a shock, but just because somebody claims to have a high school diploma or college degree does not mean that they do. Right or wrong, a lot of employers place emphasis on higher education degrees and because of this some job candidates will list degrees that they have not earned in order to be considered for employment or will acquire a degree from a Diploma Mill. "Diploma or degree mills come in many guises. Some degree mills blatantly offer

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

to sell a degree and perhaps a transcript from a legitimate school. Others can be easily recognized by promising that an applicant can receive a degree in a very short period of time, sometimes as little as five days" (Council for Higher Education Accreditation, 2007). Identifying the "bogus" degrees is not always easy either as skilled operators create websites, register phone lines and even offer class rings. In addition, with the expansion of legitimate universities who offer degrees online, and the fact that not all legitimate universities are accredited, the water gets even murkier.

One thing that you can do to attempt to verify a degree is to validate that the dates of enrollment or graduation don't conflict with other dates or addresses that you have been provided. In other words, did the individual receive a degree from a university on the east coast (that does not offer on line degrees) while living and working on the west coast? Also, search the internet for mention of the university to see if there is information regarding its legitimacy. If possible, contact the university and have them validate dates of attendance and degrees conferred. If it is supposed to be a physical university, map it as described above.

Personally I don't believe that a college degree guarantees that one individual is a better candidate that another (this coming from an individual who has earned multiple college degrees), however I do believe that if you are the type of person who will falsely claim to have earned a college degree then I have reason to doubt your trustworthiness.

Work History

Look at the individual's work history carefully, perhaps even taking the time to plot the employment dates on a time line along with the individual's graduation dates. Look for inconsistencies,

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

overlaps or gaps between jobs and degrees. If desired (and with the individuals permission) you can contact the previous employers to confirm that the employment dates, position and responsibilities have been reported accurately. As an additional check look up the contact information yourself, rather than just accepting what the individual has provided you, and validate the address as described previously. Some ideas of things to look for may include, but are not limited to:

- Did the person claim to be working in one state while they were supposed to be attending a University hundreds or thousands of miles away?

- Are there gaps in the timeline that might indicate that the individual has failed to report something?

- Does it appear that the individual worked for different employers simultaneously?

- Is there a pattern of very short employment periods?

- Did the individual claim to accomplish something, or have a responsibility, that is not consistent with the position or length of employment?

These are just ideas to help you get your own list started and you will have to evaluate the results for yourself. It may or may not be significant that the individual has been employed by eight different companies in the last two years or that they were employed by two different companies at the same time. After all, you are the one who has to determine whether you feel that the individual can be trusted.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Employer and Character References

First, I'm not going to try to cover all of the legalities behind reference questions - this paper is long enough as it is. The essential thing to bear in mind is that all of your questions should be seeking information that is pertinent to the job for which the individual is being considered. Of course, one of the likely job requirements is that the individual be considered trustworthy, so the possibilities abound.

Character References (or Personal References) are non-work related contacts who have been requested by the individual to vouch for them and whose contact information has been provided to you on an application or additional information form. These may be neighbors, friends or perhaps even somebody who knows the individual through some form of volunteer or community organization. As to validating the legitimacy of the reference, there is only so much that you can do. As we saw above, you could attempt to validate that the phone number is associated with the reference's name and that the address is appropriate for the persons association with the individual. As an example, if the reference is supposed to be somebody who volunteers for the same local fire department as the individual, however one person lives in Florida and the other lives in Oregon, then perhaps you should raise an eyebrow. One advantage to a Character Reference over an Employer Reference could be in that the Character Reference has fewer legal restrictions on the information that they can provide on the individual.

Employer References are individuals with whom, or for whom, the individual has worked. They could be for the individual's current job or they could be for past jobs and they can either be provided by the individual or, with the individuals permission (another thing for the waiver), they could be drawn from the individuals employment history.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

One way to validate an Employer Reference could be to research the company on the internet and call the company's operator instead of using the direct number provided by the individual. Sometimes this will work, and sometimes you will be referred to the Human Resources Department. In addition, some companies have rules regarding what an employee can say – some employees follow these rules, some don't (I'm not going to address tones, slips, insinuations, etc). Regardless of whether you are contacting a character Reference or an Employer Reference, start off by introducing yourself and describing the position that the individual is being considered for.

- Tell the person some of the characteristics which are important for this position and ask them if they know of any cause for concern.

- Ask questions of previous employers to determine if the individual accurately reported previous job dates, roles, responsibilities and performance.

- Ask if they missed work, made deadlines, were frequently late or exhibited poor job performance,

- Ask if they would hire them again

- As a final question, ask them if there is anything that you haven't asked that they would like to share with you.

Social Security Number (SSN)

While an individual's Social Security Number can be validated for free through the Social Security Administration (SSA) website (http://www.socialsecurity.gov/bso/bsowelcome.htm) for the purpose of completing Internal Revenue Service forms, legally this service

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

shouldn't be used for a background investigation. Words of caution from the SSA website:

- You may not verify someone's name and Social Security number until after you have offered him or her a job.
- Social Security will verify Social Security Numbers (SSNs) solely to ensure that the records of current or former employees are correct for the purpose of completing Internal Revenue Service Form W-2 (Wage and Tax Statement).
- Anyone who knowingly and willfully uses SSNVS to request or obtain information from Social Security under false pretenses violates Federal law and may be punished by a fine or imprisonment, or both (Social Security Agency, 2007).

Multiple other "free" services that can be located on the internet don't actually validate that a SSN is assigned to an individual, but rather they use the significance of the different SSN groupings (AAA-BB-CCCC) to determine what geographical area and in what year range the SSN was issued (which is not necessarily where and when the individual was born). So how do all of the agencies on the internet that offer, for a fee, to validate an individual's SSN legally get this information? The answer is through an SSN Trace. "A social security trace is a report that will return all current and reported addresses for the last 7 to 10 years on a specific individual based on his or her social security number. If there are alternate names (aliases or also known as [AKA]) these are reported also....The SSN Trace report is derived from credit bureau records and follows a standard format. The sources include applications for utilities (telephone, electric), credit checks for loans and/or credit cards, and qualification for rental agreements" (4nannies.com,

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2007). Those are the same Credit Bureau reports that we discussed earlier and that we will now discuss in more depth.

Credit Reports

There are three National Credit Reporting Bureaus (Equifax, Experian and Trans Union) that collect information on individuals and companies and they don't share their data with each other. I assume that this is to limit the effect of incorrect information and allow confirmation of correct information, however, as I have stated previously, I have been wrong before. Each of the three Bureaus offers various service packages that, for a fee, address a wide range of business needs from Credit Reports (also known as Consumer Reports) to demographic marketing solutions. The service that we are interested in, the Credit Report, can include but is not limited to, the following information:

- Personal Information – Personal Data, SSN, current and previous addresses, type of residence and employment history.
- Account Information - Summary and detailed account information.
- Inquiries – Companies that have requested or viewed the individuals credit information.
- Collections – Account that have been turned over to collection agencies.
- Public Records – Bankruptcies, liens, garnishments and other judgments.

Please remember that, as described earlier, not all of this information can be utilized in making employment or promotion

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

decisions and that there are specific conditions and rules under which any of the information can be used. But there is much that can be utilized to assist us in making the vital decision of whether we feel the individual can be trusted. We can verify the individual's SSN, addresses and employment history as well as evaluate whether the individual has a history of meeting their financial obligations. We might even look for indications that they are potential targets for financial corruption such as "is the person deep in debt or are they living beyond their probable income?" While perhaps not definitive or decisive by itself, this information may help you make your "trust" decision.

Wondering what information your credit report contains? You can easily, and are highly encouraged to, obtain a free annual Credit Report on yourself from each of the three National Credit Reporting Bureaus individually or by visiting https://www.annualcreditreport.com/cra/index.jsp.

Criminal Records

A multitude of firms advertise that they will conduct a criminal background check for you but it behooves you to understand the limitations that exist so that you will better understand the quality and reliability of the information that you are delivered. Anybody who watches TV or movies may believe that a criminal background check is a simple matter of punching an individuals name into a tool that searches a Comprehensive National Database and reports every arrest and conviction related to the individual. However no such Comprehensive National Database exists and even if it did it would not be able to provide all of the data that you might like to see. The closest thing to such a Database, that non-government entities may get access to, is the National Criminal File and it is not as extensive or complete as you may be led to believe. In order to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

understand this better you need to understand a little bit about the way that Criminal Records are generated and recorded as well as what resources are available to search these Criminal Records. The Virtual Chase website offers the following write up:

> During the past year a new type of pre-employment background check called the National Criminal File (NCF) became available. There are 38 to 50 states included, and the number of records in these three NCF databases ranges from 60 million to as many as 133 million. While those numbers sound impressive, any company that utilizes the National Criminal File as their primary means of checking for criminal records should read the fine print.
>
> There are four different kinds of records, all of which are referred to as "criminal records."
>
> - Arrest Records—law enforcement records of arrests.
> - Criminal Court Records—local, state or federal records.
> - Corrections Records—prison records.
> - State Criminal Repository Records—statewide records made up of arrest records, criminal court records and correction records.
>
> This article discusses the differences among these records and how they come into play with the National Criminal File.
>
> **Criminal Justice System Basics**
>
> We have said that there are four different kinds of criminal records. They come from different parts of the criminal justice system. When someone is arrested the arresting agency completes an arrest report, which becomes an arrest record. Then, the defendant is arraigned and tried in criminal courts. These records are referred to as criminal court records. At the conclusion of the trial, the case will either be dismissed or the defendant will be convicted.
>
> **There is no such thing as a nationwide criminal records check.**
>
> When a conviction occurs, there are several possible sentences. For example, the defendant may have to perform community service, pay a fine, or might be placed on probation. Sometimes the defendant will be sentenced to incarceration. When an individual is incarcerated for a

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

> misdemeanor, they will be sent to jail, rather than state prison. If, however, it is a felony conviction, the defendant may be sent to either jail or prison. Generally only the most violent felons, serious drug abusers, and repeat offenders are sent to prison. Records of imprisonment in state prison are called corrections records. Arrest records, criminal court records, and correction records are sent to the state criminal repository.
>
> **The Mythical Nationwide Criminal Check**
>
> While the National Criminal File search sounds extremely good, the reality is that there is no such thing as a nationwide criminal records check. Even the FBI database is not truly nationwide. The FBI database (NCIC) does not include most misdemeanors. Many records never make their way to the FBI because the records must be sent from the county to the state and from the state to the FBI, and frequently there are breakdowns in the process. Nevertheless, the NCIC database is the closest thing that we have to a national criminal database, and it is far more comprehensive than the NCF.
>
> The vast majority of the data included in the NCF is made up of corrections records. Again, only the most serious criminals are sent to state prison (The Virtual Chase, 2005).

So in order for a National Criminal Database to be ”complete and accurate” every police department and every court system would have to send every arrest record, every criminal court conviction and every local and county corrections record to the appropriate State level organization where they would have to be combined with the state corrections records and properly cross referenced by a distinct identifier (such as SSN rather than a last name). But every state has different records keeping standards (as well as enforcement of those standards) and so this situation does not always occur.

As such in order to perform a truly thorough and complete criminal background investigation it would literally be necessary to personally visit every locality where an individual might have been arrested, convicted or incarcerated to manually search their records.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

If the individual was born and raised in one locality, has never left that locality and (if applicable) still utilizes their maiden name, this may be plausible. However this is not a likely scenario. Realistically you are probably limited to searching the available on-line records for the states and counties where you are confident that the individual has resided. A good starting point for such a search is the BRB Publications Incorporated Free Public Records Sites webpage (http://www.publicrecordsources.com). From this one site you can find links to many state and county sites where you can perform free searches for various criminal records (among other things). Whether you decide to perform your own search or to purchase a criminal background report from a vendor who has applications that automate access to as many state and county search engines as possible, the information that you receive is not guaranteed to be complete or accurate, and now you understand why.

What Information should you trust

So once you've gone to all the effort to gather or verify information, what information can you trust? As suggested in the Criminal Records section above, you can't always (shock!) trust the government and you can't always (shock!) trust the individual. The fact that you have a right to dispute your Credit Report (as discussed in the FCRA section) should indicate to you that they are known to contain incorrect information as well. And as we explained above, many of the background checks available on the web utilize the above mentioned records to compile their reports.

To illustrate this point I will use as an example the report that I ordered on myself from one of the more prominent background report companies on the web. I provided them with my name, current address, SSN and DOB and requested a background report that would include personal public records data, address history, single state

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

civil judgments and criminal check, nation wide state and federal criminal check. The resulting 104 page report that I received was "interesting" to say the least. For starters, though I have never owned property with my brother, nor lived in the state that he currently resides in, his residential tax records were listed as my primary residence (so that's what a split level house on a golf course is worth!). And while several of my previous addresses were returned there were also several addresses that I have never lived at (is that where all that lost mail went?). But the most eye opening (and sickening) part of all was that almost 100 pages of the report contained criminal records listing all sorts of terrible crimes thought to be committed by individuals (other than myself, of course) of various ages, races and possibly genders, by the name "Timothy Cook." We Timothy Cook's really need to police our ranks better.

To complicate matters even more, there are diploma mills and individuals who, for a fee, will falsify records, hack databases or even provide false references. Face it, people lie, governments aren't perfect, reports contain errors and there are even businesses that help people lie and cheat. So what information should you trust? I can't tell you - that is a decision that you are going to have to make based on your evaluation of every specific situation. All I can suggest is that you view all information as suspect until it can be corroborated or validated and that you always provide the individual with a chance to refute negative or conflicting information.

Summary

Background investigations are a vital step in both establishing the inner security perimeter of your Defense in Depth and in protecting your firm from negligence lawsuits. They need not be overly intrusive or expensive and can either be conducted internally

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

or by one of many companies that specialize in performing Background Investigations and are up to date on the legalities in the states in which you operate. The records accessed during the course of a BI are mostly public information and the use of this information is governed by federal and state laws.

While not everybody in your employ may need to have a BI conducted on them, those who will be provided access to your company's most valuable resources probably do. The ultimate purpose of a BI is not to provide a guarantee that an individual is honest, but rather to provide you with adequate information to make the determination as to whether you believe the individual can be trusted with your firm's valuable resources. It helps to confirm information that an individual provides to you voluntarily and potentially to uncover information that they have failed to provide.

Finally, always remember that whether you decide to outsource Background Investigations or to conduct them yourself it is important to obtain a signed waiver of rights, consult legal consul and to always provide the individual with an opportunity to refute any negative or conflicting information utilized in your decision making.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

References

4nannies.com (2007). About the Social Security Number Trace. Retrieved May 10, 2007 from http://www.4nannies.com/info/SSNTrace.cfm#top

American Psychological Association (2007). *Reference Example for Electronic Source Materials*. Retrieved March 5, 2007 from http://www.apastyle.org/elecsource.html

Computer Security Institute(2003). 2006 CSI/FBI Computer Crime and Security Survey. Retrieved March 9, 2007 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Computer Security Institute (2005). 2005 CSI/FBI Computer Crime and Security Survey. Retrieved March 9, 2007 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf

Computer Security Institute (2006). 2006 CSI/FBI Computer Crime and Security Survey. Retrieved March 9, 2007 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Council for Higher Education Accreditation (2007). Degree Mills: An old Problem and a New Threat. Retrieved May 11, 2007 from http://www.chea.org/degreemills/frmPaper.htm

Creditreporting.com (2007a). Fair Credit Reporting Questions and Answers. Retrieved March 21, 2007 from http://www.creditreporting.com/fcraqa.html

Creditreporting.com (2007b). Fair Credit Reporting Act and Your Credit Report. Retrieved March 21, 2007 from http://www.creditreporting.com/fair-credit-reporting-act-law.html

Electronic Privacy Information Center (2003). The Privacy Act of 1974. Retrieved April 11, 2007 from http://www.epic.org/privacy/1974act

Federal Bureau of Investigation (n.d.). Security Clearance Process

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

for State and Local Law Enforcement. Retrieved February 20, 2007 from http://www.fbi.gov/clearance/securityclearance.htm

Hurley, Becky (2005). Securing a Security Clearance May Not Be Such a Simple Task. Dolan Media Newswires. Retrieved March 15, 2007 from the findarticles database http://www.findarticles.com/p/articles/mi_qn4190/is_20050916/ai_n15354599

Niznik, John Steven (2003). Security FAQs. Retrieved February 20, 2007 from The New York times Company at http://jobsearch.about.com/od/governmentjobs/l/aa_security.htm

Personnel Policy Service, Inc. (2007). You Can't Ask That: Application and Interview Pitfalls. Retrieved April 19, 2007 from http://www.ppspublishers.com/articles/application_interview.htm

Powers, Rod (2007a). Security Clearance Secrets: Part 1, Page 3. Retrieved February 20, 2007 from The New York times Company at http://usmilitary.about.com/cs/generalinfo/a/security_3.htm

Powers, Rod (2007b). Security Clearance Secrets: Part 2, Page 3. Retrieved February 20, 2007 from The New York times Company at http://usmilitary.about.com/cs/generalinfo/a/security2_3.htm

Privacy Rights Clearinghouse (2007). Fact Sheet 16: Employment Background Checks. Retrieved April 6, 2007 from http://www.privacyrights.org/fs/fs16-bck.htm

Purdue University (2007). APA Formatting and Style Guide. Retrieved April 20, 2007 from http://owl.english.purdue.edu/owl/resource/560/01/

Riley, Chris (2003). How Well Do You Know Your Systems Administrator. Retrieved March 5, 2007 from the Global Information Assurance Certification website http://www.giac.org/certified_professionals/practicals/gsec/2338.php

Social Security Agency (2007). Social Security Online: Business Services Online. Retrieved May 10, 2007 from SSA website

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

http://www.ssa.gov/bso/services.htm

The Dice Company (2006). Security Clearance Frequently Asked Questions. Retrieved March 14, 2007 from http://www.clearancejobs.com/security_clearance_faq.pdf

Tucek, William T. (2003). Identifying and Mitigating Risks of Information Technology Outsourcing. Retrieved March 5, 2007 from the Global Information Assurance Certification website http://www.giac.org/certified_professionals/practicals/gsec/2400.php

United States Department of Justice (2004). Freedom of Information Act Guide, May 2004: Introduction. Retrieved March 19, 2007 from http://www.usdoj.gov/oip/introduc.htm

Virtual Chase, The (2005). Not All Criminal Records Checks Are Created Equal. Retrieved May 16, 2007 from http://www.virtualchase.com/articles/criminal_checks.html

Wikipedia (2007). Freedom of Information Act (United States). Retrieved April 9, 2007 from http://en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States)

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced