Hiring Ex-Criminal Hackers

Ed Skoudis, CISSP

Making their way, the only way they know how.
That's just a little bit more than the law will allow.

— Waylon Jennings, “Good Ol' Boys”
Theme song from Dukes of Hazzard

Suppose someone applies for a system administrator job, or, better yet, an open slot on your computer security team. The applicant is eminently qualified for the position, having wizard-like skills on the exact operating systems deployed throughout your organization. You need his skills, big time. However, the candidate poses a bit of a problem. This otherwise-stellar applicant has a bit of a spotty record with the criminal justice system. By spotty, I mean that your potential hire was found guilty of hacking a Fortune 500 company and stealing some sensitive data. He did the crime, but he has also done the time.

Should you still consider such a person for a position on your security team? Or, should you let bygones be bygones and just move forward? Some companies shy away from such individuals immediately. Others take a “Don’t ask... Don’t tell” stance. Still others actively embrace such people for their great skills. If your organization hires an ex-criminal hacker, would you be legally responsible if he damages a customer or supplier’s computer systems? You could be found guilty of negligent hiring, whereby an employer is liable for taking a hiring risk and exposing customers, suppliers, and other employees to it.

This chapter analyzes the issues associated with hiring ex-criminal hackers so you can think through your own organization’s approach to this issue. The chapter looks at both sides of the problem, and then the author states his opinion on the matter, for what it is worth. While the author attempts to evenhandedly argue both sides of this topic, keep in mind that the author does not necessarily agree with all of these arguments. Instead, the concepts raised are those most often advanced by proponents on either side of this divide.

The discussion in this chapter does not refer to non-criminal hackers. Remember, as used in the computer underground, the term “hacker” does not by itself imply that the person has done wrong. People who have hacking skills may have acquired them completely lawfully, by studying computer security or conducting legitimate penetration testing against consenting targets, such as their employers or customers. There are many of these “white-hat” hackers in the information technology business. The author himself falls into this white-hat category, as do many others, and would like to think we are very hirable without concerns.

This chapter analyzes the question of whether to hire hackers who have an actual prior criminal conviction, or are known to have been involved in criminal activity but may have not been prosecuted (yet). We refer to them as ex-criminal hackers because they were either busted and did some time in jail or are known to have committed crimes. In other words, we are talking about actual former black hats or deeply gray hats.
Why This Matters

One might wonder if this analysis really matters that much. Actually, it really does (of course I think that... I would not be writing about it if I didn’t.) But, think about it. Information technology (IT) carries and stores the lifeblood of most organizations today: information. The people who run this technology have tremendous access to the most sensitive information an organization has: personnel employment and health records, sensitive customer data, legal and regulatory compliance information, comprehensive financial results, and perhaps even launch codes. Just to keep the organization running, the IT department often acts as a high-tech priesthood given wide-open access to the very soul of the business.

If IT has a bad egg as an employee, the damage that can be done to an organization’s finances, reputation, and very existence might be devastating. Inside personnel know how to hit an organization where it hurts, undermining technology and processes to maximize not only their own personal gain but also the damage inflicted on their target. Looking at statistics regarding computer crime compiled annually by the Computer Security Institute and the FBI, the number of attacks from insiders and outsiders is virtually the same. However, the cost of damages from computer attacks commonly perpetrated by insiders (insider net abuse, financial fraud, and theft of proprietary information) significantly outweighs the cost of attacks by outsiders. That is because insiders know how to cause trouble for their organizations.

The 2002 CSI/FBI survey also indicated that 65 percent of organizations would not consider hiring reformed hackers as consultants; 17 percent of others would consider it; while the remaining just do not know. In this author’s experience, even the 65 percent of those who say they would rule out hiring ex-criminal hackers do not have explicit policies regarding this decision or even very detailed background checks to enforce it. Therefore, even among those whose guts tell them not to hire ex-criminal hackers, many unwittingly hire them without understanding their background. Is this wise? Let us explore the case for and against hiring ex-criminal hackers in more detail.

The Case for Hiring Ex-Criminal Hackers

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not by what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can’t stop us all...

— From the Hacker Manifesto, written by “The Mentor” in the mid-1980s

This creed by “The Mentor” is still very relevant today, as it highlights many of the issues associated with hackers and the computer underground, including whether organizations should employ ex-criminal hackers. We analyze some of the issues brought up in the Hacker Manifesto, as well as related topics. The arguments for hiring ex-criminal hackers fall into three general categories: questions associated with who is really to blame, doubt about how dangerous computer attackers really are, and society’s need for exceptional technical talent.

It’s Not Really Their Fault...

I went to the lost and found department at my local shopping mall. I told the kid behind the counter that I’d lost my youthful exuberance. He said they’d call me if it turned up.

— William J. Basile, my college roommate

One of the primary arguments for hiring ex-criminal attackers involves looking at whether we can really assign blame; and, if we do, who is really at fault. First, consider the focus of our criminal justice system — reform. By definition, a penitentiary is where someone repents for past crimes, and is reformed to become a contributing member of society. After their release, they have done their time, and should be able to contribute fully to society. Harshly turning down such people from employment may doom them to perpetuate their life of crime. For crime in general, the recidivism rate is far lower when someone returns to society as a productive member.
of the workforce, especially for young people.² Turning the other cheek, as it were, may help them have a positive impact on society. They have paid for their past sins, and it is time for forgiveness. Who is a potential employer to judge when the criminal justice system has already not only judged, but punished?

Furthermore, young people commit many computer crimes in their high-school or college years. Such perpetrators are not hardened criminals; they are merely satisfying their youthful wanderlust by exploring computer systems. As with many young people, they are merely pushing the boundaries of their environment to understand how the world works. If they do not really cause much damage, can we really damn them for simply discovering vulnerabilities and pushing the boundaries of human knowledge? Is that not what being young is all about? This line of argument fills the pages of the always-interesting and often-provocative 2600 magazine.³ This self-titled, “Hacker Quarterly” magazine is published every three months and can be found in most major bookstores' magazine rack. In addition to some technical content describing attacks, the magazine also actively promotes the culture of disaffected youth exploring computers for fun and learning. According to this mind-set, these noble adventurers are not setting out to do damage, and are simply misunderstood by a society either too evil or too stupid to understand the subtleties of the computer underground.

Also, our overall society seems to encourage adventurous computer hacking. Consider recent movies like The Matrix from 1999, or its 2003 sequels. In those movies, a corrupt culture tries to stifle an innocent computer hacker who may expose its ultimate lie. In another classic hacker movie, 1983’s WarGames, a hacker is the ultimate hero, saving the world from a nuclear holocaust (which, of course, he accidentally triggered in the first place). In these and many other examples, the hackers are the good guys, trying to save the world from corruption. Does it make sense to limit job opportunities to such people simply because they have followed the lead given by our mass entertainment culture?

### Are They Really That Dangerous, or Do They Help?

Want to play a game?

— WOPR, the computer from the movie WarGames

A second and related argument associated with hiring ex-criminal computer attackers involves a consideration of the real damage done in a large number of computer attacks. According to this argument, a computer attack involves minimal real-world damage, with an attacker just exploring a network and copying some files. No lives are in jeopardy, and usually, minimal real-world losses are incurred. However, the attacker may find himself in jail simply because his case was novel and his target especially juicy. For cases with little or no real-world damage, computer attackers should be given another chance at using their skills for good.

Also, numerous people in the computer security industry have gotten started by youthful exploration of computer systems with little harm to society as a whole. Some of the most skilled computer security personnel today cut their teeth by surreptitiously breaking into other people's computers. Sure, goes this argument, now that we are all grown up, we recognize the errors of our youth. If we put everyone in jail who learned computer security by breaking into systems, we just may decimate the computer security industry. Furthermore, some of the folks who encourage tough penalties for computer crime are, in fact, hypocrites, given their own shady pasts. While such people may criticize those who were unlucky enough to get caught, they themselves were just as guilty of computer attacks when they were youngsters.

This argument is bolstered by the wonderful contributions of some high-profile individuals who have bent or even broken the law in computer and related attacks in the past. For example, consider Steve Jobs, the celebrated founder and current CEO of Apple Computer, Inc. Back in college, Jobs entered the hardware business not by selling candy-colored, easy-to-use computer systems. Instead, he made money the old-fashioned way (at least for the 1970s): he sold blue-box hardware that generated specific tones allowing users to explore or defraud the public telephone system. Although Jobs was never charged with a computer-related crime, clearly his exploits were not in the best interests of the telephone company. Yet, looking at the sum total of his activities in the computer field, Jobs has greatly improved the computer industry, helping to introduce the personal computer and then the graphical user interface to the masses, birthing Apple Computer, and then saving Apple from near extinction.

Another example involves Kevin Poulsen, one of the best journalists in the computer security industry today. Poulsen once served significant jail time for some elaborate attacks against a large California-based telephone company.⁴ But that is his past; he is now helping advance the cause of computer security as the chief editor of

© 2008 by Taylor & Francis Group, LLC
the online security news and editorial section of SecurityFocus.com. Poulsen’s past is checkered; his current stuff is extremely helpful in understanding how to and why we should secure our systems.

This argument extends to numerous other individuals. Much of the computer and Internet industries was built by people who push the limits of both technology and the law. These concerns point to the often-blurred line between computer professionals and computer attackers, the indistinct separation of white hats and black hats into a gray goo. Let’s face it, if Jobs, Poulsen, and others built their technical and business savvy, as well as our overall networked world, by illegally tapping into computers and helping others to do so, today’s computer attackers may be tomorrow’s computer security professionals, professors, CEOs, or even presidents. I can just picture the bumper stickers now — Kevin for President! Watch out!

But We Need Them...

Another area for consideration on the issue of hiring ex-criminal attackers involves our society’s need for technically sophisticated personnel. Although a recent recession has furloughed many IT professionals, people with very strong security skills remain in high demand. Looking at the vast numbers of gaping holes in corporate networks and major software packages, it is clear that businesses just cannot get enough good security people to shore up their networks against attack. Putting our best and brightest in prison and never hiring them after they have been reformed is a waste of some very valuable human capital. Given the great contribution these folks can make, as compared with the costs of keeping someone on public assistance or in prison, society as a whole benefits from having ex-criminal hackers gainfully employed.

Focusing on the computer security industry, ex-criminal hackers understand computer attacks far better than anyone else does. They truly know the hacker mind-set. While they may or may not have the best skills in conducting overall computer security architecture, such people are among the best in doing detailed penetration tests. For such testing, one needs to think like an attacker and employ the skills and mind-set associated with deep, focused analysis on ripping apart networks, operating systems, and applications. The best penetration tests are done by those who not only consider today’s known vulnerabilities, but also look deeper for new holes and exploits. Sometimes, ex-criminal hackers are the absolute best at doing this.

In fact, many of the major vulnerabilities discovered today are found by those labeled “gray hats,” people who may be in trouble with the law but continue to do computer research. If one looks beyond some of their bravado and unusual culture, these people may actually be helping the information security industry do research, understand problems, and fix vulnerabilities before the serious bad guys do. Our underlying technology is so severely feeble from a security perspective that finding and pointing out these vulnerabilities is really valuable. On a daily basis, major vulnerabilities are discovered in systems of all types: desktops, servers, personal digital assistants, routers... you name it. If it has software in it, chances are that someone has found security flaws in it, and quite often that person is a reformed, ex-criminal hacker.

Gobbles, a group of security researchers, found some major security vulnerabilities, including a significant flaw allowing complete remote compromise of Apache Web servers in mid-2002. Their brash style, together with their penchant for full disclosure including the release of easy-to-use exploitation code, have rubbed many in the computer security industry the wrong way. However, would you rather have Gobbles discover and publish such findings, or a major terrorist group or foreign country’s cyber-warfare troops exploit such holes in a massive attack against the world’s infrastructure? Clearly, full disclosure from Gobbles is the better (although perhaps not the best) alternative, as it allows us to fix our problems. Despite Gobbles’ strong gray-hat status, they have helped improve Apache’s security.

Similarly, Adrian Lamo has broken into and explored the sensitive inner networks of The New York Times, Yahoo, and WorldCom. Although he has publicly admitted that such adventures may run afoul of the law, Lamo points out how he has helped these companies secure themselves. Lamo’s “victims” have expressed gratitude for his open attitude of sharing information about his exploits with these companies before going public. By discovering flaws in our systems, Lamo, Gobbles, and many others run up against the law and in some cases explicitly violate it. However, in doing so, they ultimately improve the state of computer security by making us focus on computer problems.

Consider a biological analogy that sheds some light on this whole issue. According to recent research, if children are not exposed to any common colds while they are under age ten, their immune systems are in fact weaker as they grow up. As youngsters, they have not built up strength and immunities. In a similar way, computer attackers represent colds periodically impacting the computer industry. Just like colds, they build our defenses by making us harden our systems and deploy patches. That way, we will be much better off when
a really serious computer attack occurs. For example, when the Code Red worm spread rapidly in July 2001, it was not only a nuisance. In fact, it made many of us patch our systems and revisit our computer incident handling capabilities. In a counter-intuitive way, some computer attackers help improve computer security by actually attacking our systems in violation of the law.

On top of that argument, we also have to consider what happens if we do not employ the ex-criminal attackers in helping improve computer security. We may very well miss some big vulnerabilities. If ex-criminal hackers cannot use their skills for good, they will use them for evil. By hiring such individuals, the computer industry can keep some of our best and brightest people focused on improving computer security, rather than unraveling the network and systems from underneath us. If these people are gainfully employed in the computer business when they discover vulnerabilities, they will be more likely to share their findings in a responsible way, disclosing it to the appropriate vendors and helping to seek a positive solution for the problem.

One analogy for this situation involves the dilemma over Russian nuclear scientists. After the end of the Cold War, these brilliant researchers were no longer needed to design and build bombs for the now-defunct Soviet Union. Many people fear that, with hard economic times in Russia and a skill set that cannot be readily applied to other jobs, these scientists may help rogue states or terrorists fulfill their nuclear attack fantasies. Because of this concern, the international community has set up programs to employ such scientists in managing and even safely destroying nuclear stockpiles. In a similar way, if we do not utilize our ex-criminal hackers, the criminal underground may hire them to conduct seriously nasty attacks. A computer attacker who has served jail time may have made contact with non-computer criminals while in prison. If the ex-criminal hackers cannot find a means to support themselves using their computer skills because they are blackballed from employment, they may turn to their “friends” from prison for funding. Nastier computer attacks result. By hiring such individuals and directing them toward good, we help to alleviate this sort of problem.

The Case against Hiring Ex-Criminal Hackers

As one might guess, not everyone agrees with the line of arguments above (now, there is an understatement!). So, how do critics respond? Let us take a look at their critiques, lining them up in the same order as the arguments presented above.

But It Really Is Their Fault

Ex-criminal hackers have already demonstrated that they cannot be trusted with access to computer systems. Many of them have been judged in a criminal justice system with safeguards to protect the innocent. “Sure,” goes the argument from many organizations, “we believe in reforming criminals and forgiveness in general, but it’s not our organization’s job to spread forgiveness and improve the world by putting ourselves at risk.” Most organizations are in business to either make a profit or deliver services to a constituency. Management and employees of these organizations have a fiduciary responsibility to protect customers, employees, and shareholders from unnecessary risks. Hiring ex-criminals into an information technology department and giving them access to a network with sensitive data to help make the world a better place is not a palatable trade-off for most organizations.

Not hiring ex-criminal hackers can also have a deterring effect. Especially in cases of computer crime involving young people, strong penalties will discourage them from turning to a life of crime. Indeed, right now, some elements of the computer underground perversely joke that if they do ever get busted, they will do their time in jail and become highly paid security consultants after they get out. As a society, it is just not right to reward malfaeance with the promise of six-figure salaries after a year or so in prison. By reversing this logic and making sure that committing computer crime means that you seriously damage your career in technology, we can dampen young people’s interest in computer crime. Instead, they may turn their skills to responsible and beneficial computer research, rather than breaking into systems.

Additionally, the idea that it is really not a criminal’s fault because *The Matrix* and *WarGames* glorify hacking just shifts blame from the legitimate perpetrator. There are numerous movies that glorify lewd behavior or even mass murder, but we do not decriminalize these activities. Even Robin Hood preached stealing from the rich and giving to the poor, yet we still criminalize theft. We simply do not rely on Hollywood to define our hiring practices, let alone our criminal justice penalties.

© 2008 by Taylor & Francis Group, LLC
They Really Can Be Dangerous!

Let's play Global Thermonuclear War.

— David Lightman, Matthew Broderick's character in the movie WarGames

Although it may be true that some computer security personnel and other technology industry luminaries skirted the law over the past three decades, this fact does not exonerate the current generation of computer criminals. In the 1970s, 1980s, and early 1990s, computers in general and the Internet in particular were far less important to the functioning of our society. The Robert Tappan Morris, Jr. Worm took down major components of the early Internet in November 1988. Yes, this story did make the evening news back then, but it resulted in little real damage. Today, with information technology permeating our financial, healthcare, and government systems, even a less virulent attack could cause many orders of magnitude more damage, disabling the Internet, causing vital systems to crash, and possibly damaging life and limb. Self-replicating worms, distributed denial-of-service, and highly automated computer attack tools can be very dangerous. With such technologies, the criminally minded hacker could wreak havoc purposely or even accidentally.

Sadly, the playful hacking of yesteryear is truly obsolete, now that our world is incredibly dependent on computers. It is not cute anymore. It is time for people to act responsibly with computer technology.

But We Do Not Need Them That Badly!

Let us now turn our attention to the argument about hiring ex-criminals because we really need their technical skills. True, our society really needs people with strong computer skills. However, we need employees with the proper skill set and attitude. For the vast majority of IT occupations, the skills needed to break into a computer system are not the same skills needed to defend a system from attack. Consider a system administrator, whose job it is to provide care and feeding to dozens of workstation and server systems. This job title is probably one of the most common roles in your IT organization that has daily access to very sensitive data. A good system administrator needs the following skills:

- Knowledge of how to keep machines up and running
- Insight into how the operating system functions at a fairly detailed level, including networking, a variety of services, and user-level applications
- Problem-solving proficiency to troubleshoot difficulties
- The ability to document and follow detailed processes, such as system configuration guides and back-up/restoration procedures
- Talent for writing simple scripts to automate tasks needed to keep the system running
- Understanding of how to configure systems securely, hardening them against attacks
- The ability to apply and test patches distributed by a vendor
- An aptitude for recognizing suspicious activities and reporting them to an incident handling team

Many ex-criminal hackers do not really have these basic system administration skills. As a general rule, in both the real world and information technology, it is much easier to break things than to build them up and maintain them. Some attackers can construct elaborate methods for absolutely ripping apart a system without breaking a sweat, but have not mastered the most basic ideas of how to keep the system running. Sure, some attackers may be able to write the code for a mutating kernel module to stealthily conquer a machine, but can they troubleshoot a flaky network connection while keeping hundreds of users happy? For many of these people, the answer is an emphatic, “No!” because their skills and attitudes do not match the job requirements.

I received strong confirmation of this point at the DefCon conference in August 2002. This annual hacker fest, held in Las Vegas, Nevada, includes a highly competitive Capture the Flag competition. In this game, teams of hackers, enthusiasts, and computer professionals are pitted against each other to vie for the highest score in a 28-hour hackathon. You get points by hacking into the other team's system, but lose points if they hack into your machine. Therefore, in the Capture the Flag contest, both offense and defense are critical. The contest starts your adrenaline pumping and remains very intense, as dozens of top-notch hackers from around
Hiring Ex-Criminal Hackers

The world are hammering your system simultaneously. During the contest this year, a friend of mine reflected the intensity of the sport by shouting expletives. "I know how to hack into these @#$%^ machines," he exclaimed, "but darned if I can stop someone else from getting into my own box!" He had attack skills, but his defense was not up to snuff.

Now, some ex-criminal hackers really do have the skills needed to be superb system administrators, but they also carry a lot of excess and damaging baggage with them. Although employers want these skills, they emphatically do not want system administrators who know how to rip apart systems. Most organizations do not want to hire system administrators, no matter how good they are, who can code elaborate hacks if they have demonstrated in the past that they have used their skills illegally. These organizations would rather have someone who may be less gifted technically, but can do a solid job without jeopardizing the organization.

Beyond system administrators, there are some jobs that really do require computer attack skills, in particular, ethical hacking. Ethical hackers penetrate systems on behalf of the systems' owner to find holes before malicious attackers do. With knowledge of the vulnerabilities, the organizations can deploy defenses based on what the ethical hackers discover. As organizations get more serious about measuring their true security stance, the ethical hacking business continues to grow, employing thousands of very talented security personnel throughout the world. To be effective, these people need skills for breaking into computers. However, the very nature of ethical hacking jobs, with their deep access into very sensitive computer systems, necessitates very careful hiring practices for these roles. Ex-criminal hackers in such positions could be extremely dangerous. They have already demonstrated the illegal use of their skills and could use a role as an "ethical" hacker to simply commit more crimes.

Let us look at the argument that criminal attackers actually make us more secure by pointing out our weaknesses before serious bad guys do major harm. Ethical hackers can serve this same function, provided that organizations actually establish an ethical hacking function. As the computer industry sorts out the liability issues associated with unsecure software and computer attacks, ethical hacking very well may become even more commonplace than it is today. Increasingly, with companies striving to limit their liability and manage risk, ethical hacking will help to measure and enforce a standard minimal set of security practices.

Sorting It All Out

So, both sides of this argument are emphatic about the logic of their respective positions. What should we make of these arguments, and should your company consider hiring ex-criminal hackers? In this author's opinion, most organizations today should avoid hiring ex-criminal attackers. Because most IT positions do involve some level of very sensitive access, you should carefully screen your potential hires to understand any computer crime activities in their past.

However, there are a small number of job roles where computer attack skills actually come in handy: vulnerability research and reporting. Vulnerability researchers do not attack particular companies' computer systems. Instead, they look for holes in computer systems in a laboratory environment, without sensitive real-world data. Their job involves finding security problems so that vendors can fix their systems, and ethical hackers can test for these holes. Universities, software vendors, governments, security consultants, and more hard-core technical publications employ such people to find vulnerabilities and figure out fixes to the problems they discover. Here is one area where ex-criminal hackers can actually make some significant contributions. Using the analogy of the out-of-work Russian nuclear scientists who get employment helping secure or destroy warhead stockpiles, our society can actually use ex-criminal hackers for vulnerability research and reporting.

However, such employment does bring risks. These ex-criminal hackers who are now doing research have to be carefully monitored to make sure their skills are being used for good. You certainly do not want to pay people to find vulnerabilities, and have them share them with criminals, foreign adversaries, or terrorists, all the while hiding the results of their research from their employer. A careful mentor program, as described below, can really help to make sure the ex-criminal hacker's skills are being used for good purposes.

Beware! Recruiting Legal Issues Need HR Support

Before finalizing the decision of whether you would want to hire ex-criminal hackers, let us discuss some important limitations you may face in finding out where your job applicants fit on the black-hat/white-hat spectrum. When interviewing and making hiring decisions, you must keep in mind any restrictions imposed...
by your own Human Resources organization, as well as employment laws and regulations. The U.S. Equal Employment Opportunity Commission (EEOC) does not have any explicit restrictions regarding whether or not to hire ex-convicts. However, the EEOC has determined that a blanket exclusion of employees with criminal convictions could be discriminatory, in that it may have a disparate impact on minorities. Therefore, such issues are generally handled on a case-by-case basis and depend heavily on the risk and sensitivity of the particular job position. As discussed above, many IT jobs and especially information security jobs are highly sensitive, but that does not mean that you can do whatever you want on this issue. Make sure you label job requisitions for IT personnel, and especially security personnel, as being very sensitive, requiring a clean background check.

This ambiguity in laws can be a major problem in establishing your own policies. Based on the lack of clear regulations on this point, many companies prohibit interviewers from asking job applicants about criminal background activities, unless a clean slate is an explicit, bona fide job requirement. Additionally, in many companies, you can only ask about actual criminal convictions, and not mere indictments or arrests. So, you may be allowed to find out that a job applicant was convicted of unsuccessfully trying to hack into a system and steal one million dollars. However, you may not be able to find out about another job applicant who successfully stole ten times that amount, but was acquitted on a technicality. Because the former case resulted in conviction but the latter was dismissed, you may only get the useful information about the first.

Your best bet here is to check with your Human Resources organization. After all, these folks get paid to know about the laws in your area regarding recruitment and to interpret those laws within your organization. Get a copy of any restrictions on interview questions or hiring limitations in writing from your HR organization before moving forward.

Background Checks That Really Mean Something

One of the most important things you can do to ensure the trustworthiness of your employee base is good old-fashioned background checks of potential hires. Start with investigating the references included in the candidate’s resume. Some organizations just assume that the recruiter or headhunter who identified the candidate double-checked all references. Unfortunately, in the vast majority of cases, that is just not true. To conduct a thorough interview process, call each reference and verify the candidate’s background and skills. Any discrepancies could indicate a big problem that you can nip in the bud in the interview process.

Beyond calling references, you may want to consider checking with the National Fraud Center (http://www.nationalfraud.com) or other background checking services to see if they have any records indicating fraudulent activity by the interviewee. These services are available for a nominal fee and can provide significant value to an organization. A record with the National Fraud Center is a significant red flag in the hiring process.

Although it has less value, you also may want to check the credit history of the potential employee. Credit histories have less value in the employment process simply because a large debt load and even a history of failure to pay debts may simply indicate that person really just needs a job. Credit problems do not necessarily indicate the risk factor of a potential hire. Carefully consider your policy on credit checks, and document in writing how you will use this information in your hiring decisions. What would you do if someone has bad credit? Would you not hire them? You may determine that credit checks do not really provide you the information you need to make hiring decisions.

Many companies also perform drug testing before any new employees can start a job. While some people consider these tests invasive, they are becoming quite commonplace. (I personally do not think such tests are very persuasive in determining someone’s criminal background with respect to computer attacks.)

Reference checks, fraud reviews, credit checks, and drug tests are not enough to ensure the trustworthiness of employees for extremely sensitive job positions. Consider ethical hacking consultants who are paid to break into the networks of clients who request penetration tests. These employees have access to the keys to their clients’ computers, and permission to storm the castle looking for valuables. Likewise, the leaders of an information security team and chief system administrators have access to all information stored on an organization’s computers. For these highly sensitive positions, when possible, hire only people that you have known for at least one year. For these tasks, promote from within, or use people whose backgrounds you have personally witnessed for over a year to ensure you can trust them. Such a policy can obviously limit the speed of growth of your organization, but it is a good start in establishing the trustworthiness of the top of your IT and security groups.
Establish a Mentor Program

One of the most effective things you can do to help detect suspicious activity by new employees in an IT organization is to develop a mentor program. After doing strong reference and background checks, assign every new employee a mentor who is a more senior, trusted member of staff. Each new hire should get a mentor for six to twelve months. Mentors are officially tasked as part of their job description with supporting new employees in their transition to the company.

In addition to helping the new employee, the mentor also acts as the eyes and ears of the company. The mentor can ensure that the new employee has the skills and attitude necessary to do the job, without exposing the company to risk. If mentors suspect that new hires have ill-will toward the company or are conducting insider attacks, they should report their concerns to management. This is not to say that mentors should be Big Brother, silently stalking every move of the new hire. However, mentors should have general knowledge of the activities of their assigned new hires. Not only can mentors help improve security through detecting and even preventing insider attacks, they can also be quite helpful in improving the productivity of new employees by getting them up to speed quickly.

We Are from the Government and We Are Here to Help

If you decide to hire ex-criminal hackers and you work for a U.S.-based company, you could benefit from a program established by the U.S. Department of Labor to help lower the financial risk companies face when hiring high-risk employees, such as ex-convicts. To encourage employers to hire such people, this federally funded Bonding Program is available to employers free of charge. The Department of Labor highlights the benefits of this program at its Web site as follows:

"Jobseekers who have in the past committed a fraudulent or dishonest act, or who have demonstrated other past behavior which casts doubt upon their credibility or honesty, often experience a special barrier to gaining employment due to their personal backgrounds. Such persons are routinely classified as "at-risk" job applicants. These jobseekers, whose past life experience raises an obstacle to their future ability to secure employment, could benefit from the Federal Bonding Program. Created in 1966 by the U.S. Department of Labor, the Federal Bonding Program helps to alleviate employers concerns that at-risk job applicants would be untrustworthy workers by allowing them to purchase fidelity bonds to indemnify them for loss of money or property sustained through the dishonest acts of their employees... It is like a "guarantee" to the employer that the person hired will be an honest worker."

Keep in mind, however, that the bond only covers up to U.S. $5000 in damages. Admittedly, in a computer attack, $5000 in damages can occur in milliseconds. Still, this insurance program, which is operated for the Department of Labor by Travelers Property Casualty, may be helpful.

You can expand the coverage beyond $5000, but the additional coverage costs come out of your pockets, and not the taxpayers. Additionally, if, instead of doing interviews, you are the one looking for a job and have a spotty record, you can get bonded yourself, to help assuage any concerns a potential employer may face.

Beyond Employee Issues: Consultants and Contractors

A final but very important point to consider regarding the potential insider threat of ex-criminal hackers goes beyond the borders of your own organization. Sure, you would never hire someone who was widely known throughout the computer underground as "Death Kiddie" and served five years in prison for wreaking hacking havoc on another company, but what about the firms you hire for IT consulting or outsourcing? Contractors, consultants, or even temporary employees could easily be attacking your organization from the inside.

There have been cases where a temp gets a job with a particular organization for a few short weeks just for the purposes of installing backdoors and other hacking tools on the organization's internal systems. After the brief stint as a temp is over, the attacker covertly controls these hacking tools from the privacy of his own home. Furthermore, some of the world's largest information security consulting firms hire ex-criminal hackers.
or sub-contract their security business to ex-criminals. These people may be assigned to your ethical hacking exercises, firewall deployments, or security design tasks if you contract for consulting services from such companies. Do you trust these people? Do their hiring practices regarding ex-criminal hackers meet your own internal policies?

To deal with this problem, you need to be aware of the threat and require your contractors and temp agencies to carefully screen the applicants they send to your company. Similarly, before signing a contract for a project with a consulting company, ask about the consultant's hiring practices with respect to background checks and employing ex-criminal hackers. Make sure that your consultant's answer to this question lines up with your own company's philosophy and policies.

**Conclusion**

Most information security organizations do not pay much attention to the criminal backgrounds of their own employee base. You should carefully consider what impact such backgrounds should have on your hiring process, and coordinate your explicit policies with your Human Resources organization. Do not shun ex-criminal hackers for every job, but instead, carefully consider the particular job requirements and risks. By carefully structuring your own hiring program, as well as selecting contractors and consultants with a similar philosophy, you can make sure your organization is properly protected.

**Note**

1. Kevin Mitnick, noted computer attacker of the 1980s and early 1990s, served a lengthy jail sentence. During his incarceration, a significant movement sprung up trying to get Mitnick released. Spearheaded by 2600 magazine, this movement is recognized for its widespread distribution of "Free Kevin" bumper stickers. For more information, see References 5 and 6.

**References**


2600 Magazine, subscription information online at [http://www.2600.org/magazine/](http://www.2600.org/magazine/).


