

CHAPTER 6

MANAGING HUMAN RESOURCES

NOW THAT YOU HAVE PHYSICALLY SECURED your territory, it's time to allow people — invited guests, of course — to come in. However, it's a worn-out cliché that people make up the weakest link in any security program. That is, people are unpredictable and more likely to be manipulated than any hardened machine. So, no matter how strong your technical defenses are, an inside employee who reveals unauthorized information defeats every security control that you have worked so hard to establish.

Considering that most attacks against your network will come from people trying to con their way in — that is, from social engineers — and that of those, most will come from insiders within your organization, careful hiring is equally as important as locking down your systems by technical means.

Unlike the technical guidelines in this book for which the settings are clearly black or white, the guidelines in this chapter provide more of a best approach than a precise tool. They offer a good measure of protection but are far from foolproof.

**Tip**

It isn't always easy to tell who is likely to be manipulated or by what and when. Whenever possible, a technical security control — which can be precisely monitored and tweaked — is more favorable than a fickle human control.

The general spheres of human-resource management that relate to security are the following:

1. Hiring policies
2. Termination procedures
3. Strategies for defeating social engineers

Hiring Policies

Managing human resources begins even before a new employee walks through the door for the first time. For security reasons, follow the pre-employment and employment procedures that are listed here:

1. Prior to employment
 - 1.1. Thoroughly review the resume and employment application.
 - 1.1.1. Verify all employment for the past five years.
 - 1.1.2. Look for any unusual or unexplained gaps.
 - 1.1.3. Verify details — including dates.
 - 1.1.3.1. University and graduate-school education.
 - 1.1.3.2. Military service and discharge details.
 - 1.1.3.3. Licenses, certifications, professional designations, and professional memberships.
 - 1.1.3.4. Special skills. (Does he or she really speak French as claimed on the resume?)
 - 1.2. Verify and call all references.
 - 1.2.1. People generally supply references who will provide glowing recommendations, so don't rely on them as the sole criteria for employment.
 - 1.3. Screen the potential employee.
 - 1.3.1. Drug tests

1.3.2. Criminal-background check

1.3.3. Credit report (useful mostly for verifying employment)



Tip

Some fraud convictions carry sentences of under two years. Such a short gap can easily be papered over on a resume and go unnoticed. Be sure that the applicant really worked where claimed and wasn't an involuntary guest in a state or federal penitentiary.



Tip

The eternal question: Should you hire that so-called reformed hacker? He seemed so charming and sincere in the interview; she did so cleverly figure out how to gain access to your computer network. And they sure seem to know an awful lot about you and your operation. However, the short answer is no. Although there are those who have, or can be, reformed, no shortage exists of good hacking types (in other words, skilled IT security professionals) who have always stayed on the right side of the law. Still, the choice is up to you. Just be aware of the risk if you choose to hire that ex-felon.

2. During employment

2.1. Review the company's IT security policy with all employees and be sure that they understand it.

2.2. Make adherence to security policies a part of the regular or annual performance review.

2.3. Reward employees for following security procedures.

2.4. Conduct regular training programs to increase security awareness.

2.4.1. Include role playing or other methods that teach employees how to spot potential social engineers and hacking attempts.

2.5. Provide a single point of contact — either one individual or a team that rotates on-call responsibilities among its mem-

bers — where employees can confidentially report security breaches.

- 2.6. To minimize panic and the inadvertent spreading of hoaxes, advise employees not to spread rumors about viruses or other attacks that were not received from authoritative sources.
- 2.7. Supply employees with regular bulletins about attacks that they should be on the lookout for.
- 2.8. Be sensitive to company changes that might cause a disgruntled employee to release internal information. Deal with these situations immediately and don't let them fester.
 - 2.8.1. Changes in job roles or titles
 - 2.8.2. Pay cuts or freezes
 - 2.8.3. Pending layoffs
 - 2.8.4. Mergers and acquisitions
 - 2.8.5. Sudden or frequent reorganizations
 - 2.8.6. Unfavorable media attention toward the company

Termination Procedures

You do the best to hire the best, but even then, employees sometimes need to be terminated. Regardless of whether the reason is performance-based or due to business losses, you should employ the following safeguards to protect your IT environment:

1. Review all your termination procedures with the legal and human-resources departments, and obtain their approval.
2. Take the following steps prior to terminating an employee:
 - 2.1. Inventory all systems, networks, applications, and data that the employee has access to.
 - 2.2. Check whether any unauthorized or rogue hardware or software exists on the employee's systems.
 - 2.3. List all the employee's user and administrative accounts.
 - 2.3.1. Particularly note any administrative accounts that include special privileges.
 - 2.4. Check whether any orphaned accounts exist, and if so, trace their ownership. If they are no longer being used, shut them down.

- 2.5. Coordinate the termination date and time with the IT-security, building-security, and human-resources departments. If possible, plan for a time when the system will not be busy, so the IT staff can disable the employee's accounts without distractions.
3. Quickly take the following steps at the moment of termination (before the employee is out the door, if possible):
 - 3.1. Remove all physical access devices (badges, ID cards, access tokens, keys, and card keys) from the employee's possession.
 - 3.2. Remove any network-access software, such as VPN clients and RAS software, from the employee's possession.
 - 3.3. Lock out access to the employee's workstation.
 - 3.4. Cancel and remove all system and network accounts.
 - 3.5. Escort the employee from the premises.
4. After termination, be sure that the IT staff checks the logs of the previously inventoried systems for any entry attempts by the terminated employee.
 - 4.1. Add rules to any Intrusion Detection Systems for checking the same.
5. If the person was employed either by the IT department or as a software developer with access to restricted systems, create backups of network configurations and crucial applications or data. In case of sabotage, you will then be able to quickly rebuild the damaged network or system.

Strategies for Defeating Social Engineers

Sure, you want to do an outstanding job and it is part of your job to be helpful, but resist the temptation to provide more information than requested, especially to a stranger. Comply only with the matter at hand, and stick to the part that is related to your specific job function. Remembering that the three key principles for defeating social engineers are verify, verify, and verify, be sure that all employees abide by the following guidelines:

1. If you receive an unsolicited or unexpected telephone call, check up on the caller.
 - 1.1. If you have caller ID, check whether the call is internal or external.
 - 1.2. If the call is internal, perform the following procedures:
 - 1.2.1. Verify the caller's identity.
 - 1.2.2. Check whether the caller is listed in the company directory.
 - 1.2.3. Phone the caller's supervisor to verify the caller's request.
 - 1.2.4. Keep in mind that an internal call is not necessarily safe. An off-site attacker can manipulate the phone system to appear as if he or she is calling from the premises. Or, an attacker could be on the premises, having used a prior ruse to gain entry.
 - 1.3. If the call is external, perform the following procedures:
 - 1.3.1. Get the caller's full name, company name, and return phone number.
 - 1.3.2. Verify that the return phone number matches the caller-ID display.
 - 1.3.3. Verify that the caller will allow you to call back later at the given number.
 - 1.3.3.1. The caller might simply hang up here, and you have just foiled a potential scammer!
 - 1.3.4. Phone the company that the caller claims to represent and verify that he or she does, in fact, represent that company.



Tip

Always verify the identity of any caller — even if that person claims to be the CEO or another high-level executive in the company. If the company takes security seriously, you will be rewarded for your alertness and not considered obstinate. Legitimate requests by upper management — even during a business emergency — are always handled through proper channels.



Tip

Skilled social engineers have done their homework and can sound just like insiders. They might say that they work in a distant department or in the technical-support department — and are just trying to help you out. They know company lingo and just enough of the inside scoops to sound legitimate. They may even claim another employee, including the employee's ID number, as a reference.

2. When a visitor arrives at the front desk or receptionist area, perform the following procedures:
 - 2.1. Verify the visitor's identity by asking to see an official picture ID — even if the visitor is wearing a uniform, particularly that of a delivery company.
 - 2.2. If the visitor has an appointment, call the employee to verify it.



Tip

Anyone can buy a uniform and fake ID that resemble those of even the most common delivery companies: [UPS](#), [FedEx](#), and so on. Be especially alert to unusual behavior or an unfamiliar driver — particularly at odd hours — or to a driver that tries to sneak in during a commotion. In these situations, verify by calling the delivery company, if possible.

3. Keep the following tip-offs to attempted social engineering in mind:
 - 3.1. Asking for confidential information as part of a story
 - 3.2. Claiming to be from the technical-support department and requesting a password
 - 3.3. Pulling rank, and threatening action against you for not complying with a request
 - 3.4. Being in a hurry, and rushing you to provide something according to a deadline

- 3.5. Excessively chattering to try and loosen you up, or using long and complicated stories with convoluted excuses



Important

Never give your password to anyone for any reason. This can't be emphasized enough. A system administrator, or anyone working at your company's help desk, for that matter, can access your system without your password and shouldn't need it for any reason. If you forget it or run into another problem with it, these same staff members can reset your password so that you can start from scratch.

4. Avoid succumbing to the following offers and requests:
 - 4.1. Free offers
 - 4.2. Free magazine subscriptions, or subscription offers that are cloaked in survey requests
 - 4.3. Surveys, marketing or otherwise
 - 4.4. Sales calls
 - 4.5. Sweepstakes awards, because legitimate winners are notified by registered mail
 - 4.6. School projects
 - 4.7. Requests for the name or ID of any employee, including yourself
 - 4.8. Requests for the company directory or where such information is available
 - 4.9. Requests for any company information other than the main telephone number

As nasty as some of the previous guidelines might seem, they can be real lifesavers. For example, social engineers sometimes call several people in an organization and obtain a snippet of information each time. They use the snippets to build a convincing identity that later allows them to fool their way into the company. However, if any link in the chain is broken, their gig is up. Social engineers are like cockroaches that work in the dark until someone turns on the light, and then they scatter. Be the one who turns on the light.