# Personnel Management and INFOSEC*

**By M. E. Kabay, PhD, CISSP-ISSMP†**

Crime is a human issue, not merely a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world won't stop someone from getting into your computer room if the janitor lets them in "just to pick up a listing." This paper summarizes the security implications of hiring, managing and firing personnel.

## 1 HIRING

Hiring new employees poses a particular problem; growing evidence suggests that many of us inflate our resumes with unfounded claims. Be especially careful of vague words such as "monitored," and "initiated"–find out what the candidate did in specific detail, if possible. Be sure that references are followed up at least to verify that the candidate really worked where the resume claims they did.

Unfortunately, there is a civil liberties problem when considering someone's criminal record. Once someone has suffered the legally-mandated punishment for a crime (fines, community service, imprisonment), discriminating against them in hiring may be a violation of their civil rights. Can you exclude convicted felons from any job openings? from job openings similar to areas in which they abused their former employers' trust? Are you permitted in law to require that prospective employees approve background checks? Can you legally require polygraph tests? Drug tests? You should consult your corporate legal staff to ensure that you know your rights and obligations in your specific legal context.

Even checking references from previous employers is fraught with uncertainty. Employers may hesitate to give bad references even for incompetent or unethical employees for fear of lawsuits if their comments become known or even if the employee fails to get a new job. Today, you can't even be sure you'll get an answer to the simple question, "Would you rehire this employee?"

Ex-employers must also be careful not to inflate their evaluation of an ex-employee. Sterling praise for a scoundrel could lead to a lawsuit from the disgruntled new employer.

For these reasons, a growing number of employers have corporate policies which forbid discussing a former employee's performance in any way, positive or negative. All you'll get from your contact in such cases is, "Your candidate did work as an Engineer Class 3 from 1991 to 1992. I am forbidden to provide any further information."

---

* This article is a compilation of short articles originally published in the *Network World Fusion Security Newsletter* in 2000 (archives at < http://www.nwfusion.com/newsletters/sec/index.html >). The material later served as the basis for Chapter 31 ("Employment practices and policies") in Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition.* Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

† Professor of Computer Information Systems & Program Director, BSCSIA, Division of Business & Management / Program Director, MSIA, School of Graduate Studies, Norwich University, Northfield, VT. Web site < http://www.mekabay.com >.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

It is a commonplace in the security field that some people who have successfully carried out crimes have been rewarded by a "golden handshake" (a special payment in return for leaving) and even positive references. The criminals can then move on to victimize a new employer. For the same reasons that we cannot know exactly how many crimes are carried out, we can't tell how often this extortion takes place.

To work around such distortions, question the candidate closely about details their education and work experience. The answers can then be checked for internal consistency and compared with the candidate's written submissions. Liars hate details: it's so much harder to remember which lie to repeat to which person than it is to repeat the truth. Ask experienced employees to interview the candidate. Compare notes in meetings among your staff. I recall one new employee who claimed to have worked on particular platform for several years–but didn't know how to log on. Had he chatted with any of the programmers on staff before being hired, his deception would have been discovered quickly enough. Ironically, had he told the truth, he might have been hired anyway.

Before allowing new employees to start work, they should sign an employment agreement which stipulates that they will not disclose confidential information or trade secrets from their previous employer. Another clause must state that they understand that you are explicitly not requesting access to information misappropriated from their previous employer or stolen from any other source.

The Uniform Trade Secrets Act, which is enforced in many jurisdictions in the U.S., provides penalties which are triple the demonstrated financial damages caused by the data leakage plus attorney's fees.

# 2 ONGOING MANAGEMENT

## 2.1 Opportunities for Abuse

Security managers don't have to be paranoid, they just have to act as if they're paranoid. Work with your colleagues to help you identify behavior that indicates increased risk for your organization.

Treat people with scrupulously fair attention to written policies and procedures. Selective or capricious enforcement of procedures is harassment. If you allow some of your staff to be alone with the check run but force all others to be accompanied, the latter can justifiably interpret your inconsistency as an implicit indication of distrust. Such treatment may move certain employees to initiate grievances and civil lawsuits or to lay complaints under criminal statutes.

Inconsistency reduces your effectiveness. Suppose George is known for a no-nonsense, bluff manner. He sticks to technical issues with his staff; he rarely socializes with his colleagues and almost never talks about anyone's feelings. George discovers that his chief programmer, Sally, seems preoccupied and irritable lately. What is Sally to think when George suddenly enquires sweetly about how things are at home and whether she is under any strain? It would be easy for Sally to misinterpret George's apparent concern as either an unwarranted intrusion into her private

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

life, a sexual come-on, or an accusation. George's unusual behavior could trigger alarm bells even in innocent employees.

In general, managers – not just security officers – should always be looking for opportunities to use the system in unauthorized ways – no wait, wait, I mean so they can identify areas for improving security (you silly, twisted reader, you)!

What would you do if you discovered that an employee who used to occupy your current office still had the key? You would politely ask them to give it up. No one would question the reasonableness of such a request. However, when you remove access to the network server room from a system analyst who has no reason to enter that area, you may be treated to resentment, sulking and abuse. People learn about keys when they're children; they don't extend the principles to information security. People sometimes treat access controls as status symbols; why else would a CEO who has no technical training demand that his access code include the tape library and the wiring closet?

You can overcome these psychological barriers to better security by introducing a different way of looking at vulnerabilities. When you identify an opportunity to use the system in unauthorized ways, turn the discussion into a question of protecting the person against undue suspicion. For example, if one of your employees were found to have more access to secured files than required for her job, you could explain that having such capabilities put her at risk. If anything ever did go wrong with the secured files, she'd be a suspect. There's no need to frame the problem in terms of suspicion and distrust.

With these principles in mind, be alert to such opportunities as making an employee remain alone in a sensitive area, allowing unsupervised access to unencrypted backups, or having only one programmer who knows anything about the internals of the accounting package.

## 2.2 Redundancy and Security

For most areas of information processing, redundancy is generally viewed as either a Bad Thing or an unavoidable but regrettable cost paid for specific advantages. For example, in a database, indexing may require identical fields (items, columns) to be placed in separate files (datasets, tables) for links (views, joins) to be established. However, in managing personnel for better security, redundancy is a requirement. Without shared knowledge, our organization is a constant risk of a breach of availability.

Redundancy in this context means having more than one person who can accomplish a given task. Another way of looking at it is that no knowledge shall belong to only one person in an organization.

Unique resources always put our systems at risk; that's why companies like Tandem, Stratus and others have so successfully provided computer systems for critical-task functions such as stock exchanges and banking networks. Such redundant or fault-tolerant computer systems and networks have twin processors, channels, memory arrays, disk drives and controllers.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

Similarly, a fault-tolerant organization will invest in cross-training of all its personnel. Every task should have at least one other person who knows how to do it–even if less well than the primary resource. This principle does not imply that you have to create clones of all your employees; it is in fact preferable to have several people who can accomplish various parts of any one person's job. Spreading knowledge throughout the organization makes it possible to reduce the damage caused by absence or unavailability of key people.

If a single employee is the only person who knows about a critical function in your organization, you are at risk. Your organization will suffer if the key person is away, and it may suffer if the key person decides to behave in unauthorized and harmful ways. Do you have anyone in your shop whose absence you dread? Are there any critical yet undocumented procedures for which everyone has to go ask Joe?

A client in a data center operations management class volunteered the following story. There was a programming wizard responsible for maintaining a key production program; unfortunately, he had poor communication skills and preferred to solve problems himself rather than training and involving his colleagues. "It'll be faster for me to do it myself," he used to say. During one of his rare vacations, something went wrong with "his" production program, shutting down the company's operations. The wizard was in the north woods, out of reach of all modern communications; the disaster lasted until he returned.

Not only does your organization suffer, but also Mr/Ms Indispensable suffers from the imbalance of knowledge and skill when no one else knows what they know. Some indispensables are dedicated to the welfare of their employer and of their colleagues. They may hesitate to take holidays. If their skills are needed from hour to hour, it becomes more difficult to allow them to participate in committee meetings. These are the people who wear beepers and cannot sit undisturbed even in a two-hour class. If the Indispendable's skills affect day-to-day operations, they may find it hard to go to offsite training courses, conferences and conventions. Despite their suitability for promotion, indispensable people may be delayed in their career change because the organization finds it difficult or expensive to train their replacement. In extreme cases, the newly promoted manager may find themselves continuing to perform specialized duties that ought to be done by their staff. I remember my amazement when the newly-promoted VP of information systems at a service bureau informed me that he was the only person on the technical support and operations team who was competent to reconfigure the mainframe computer.

## 2.3 The Expert in the Next Office

In this series, we are reviewing some of the implications of personnel management for information security. In the previous article, I discussed some of the security issues relating to shared knowledge. In this article, I examine the other security costs of failing to manage knowledge effectively.

"Marcie, can you spare a minute?" Marcie groans inwardly. This is the sixth time this morning someone has come in from a neighbouring office to ask her for "a minute". Each occasion lasted about a quarter of an hour. The questions all concerned MARVEL 4-5-6, on which Marcie is the acknowledged expert.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

However, Marcie is actually the Assistant to the Director of Finance, not a Technical Support specialist from the Information Center in Data Processing. Every time she's interrupted by a call for help from people in Accounting, Shipping, Engineering, and even occasionally from Data Processing, she falls further behind in her assigned work. She likes helping people, but lately she's had to stay late after the nominal end of her work day simply to make up for the time she has used acting as informal technical support to her neighbors.

Marcie may have a bad time of it unless something changes in her organization. She may be fired by her boss because her productivity drops too low according to her job description. She may burn out and quit because of overwork and criticism. Or she may cause resentment among her colleagues and neighbors by declining to help them or by complaining to her own boss and causing a ruckus. Alternatively, she may have a good time and manage to meet all the demands on her quite successfully until the DP department begins to feel threatened and someone either complains to the higher ups or begins spreading nasty comments about poor, helpful Marcie.

Being the expert in the next office is tough on the expert.

Looking at this situation from a management point of view, there are problems for the recipients of all this free aid. The longer they can persist in getting apparently free help from their unofficial benefactor, the longer they can avoid letting upper management know they need help with their office automation tools. Then when the bubble bursts and the expert becomes unavailable, managers are confronted with a sudden demand for unplanned resources. In some organizations, unexpected staffing requirements are difficult to satisfy. Managers have a hard time explaining how it is that they were unable to predict the need and budget for it.

## 2.4 TINSTAAFL

Engineers often say, "There is no such thing as a free lunch" (abbreviated TINSTAAFL) to imply that no benefit is without cost.

From a technical support perspective, even the most gifted unofficial expert is necessarily an amateur. True, there are many users whose technical knowledge of their tools exceeds that of their own technical support staff. But professional technical support consists of far more than just technical knowledge. Almost no amateur expert will

- have colleagues to discuss the problem with on a technical level;
- have backup personnel so she can provide faster service to requesters;
- search the appropriate technical manuals with the user experiencing a problem;
- have access to all the periodical information provided by manufacturers;
- document the problems carefully so as to avoid having to solve them all over again later;

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

- have access to phone in consulting services;
- determine the cause of the problem and ensure that the problem does not recur; and
- broadcast information about the problem, its workaround, and its fix to unaffected users who may benefit from the information.

In conclusion, failing to manage knowledge effectively can lead to a breach of availability (systems on which people rely may be inaccessible without a missing expert) or of utility (existing systems may not be fully exploited in the absence of a missing expert). From a security perspective as well as from a general management perspective, it is more sensible for employees to help themselves and each other by letting management know they need technical support.

If you are the Expert in the Next Office, when someone asks you for technical help in an area that isn't part of your formal job, by all means help them but let your manager know immediately that there's a support problem.

If you find yourself asking The Expert in the Next Office for technical help even though she isn't really supposed to be spending time on such problems, don't stop this time but tell your own manager that you'd prefer it to be an exceptional case and that you'd much rather have a permanent technical support team to work with.

## 2.5 Cross-Training and Vacation Time

Sometimes a person continues to be indispensable because of fear that their value to their employer resides in their private knowledge. Such employees resent training others. The best way to change their counter-productive attitude is to walk what you talk: share knowledge with them and with everyone else in your group. Make education a normal part of the way you work. Encourage cross-training by allocating time for it. Make cross-training a factor in your employee evaluations. Have discussions of current topics from the trade press and academic journals. Start a journal club where people take it in turn to present the findings from recent research in areas of interest.

Reluctance to explain their job to someone else may also mask unauthorized or illegal activity. Take for example the case of Lloyd Benjamin Lewis, assistant operations officer at a large bank. He arranged with a confederate outside the bank to cash fraudulent check for up to $250,000 each on selected legitimate accounts at Lewis' branch. Using a secret code stolen from another branch, Lewis would scrupulously encode a credit for the exact amount of the theft, thus giving the illusion of correcting a transaction error. Lewis stole $21.3 million from his employer between September 1978 and January 1981, when he was caught by accident. For unknown reasons, a computer program flagged one of his fraudulent transactions so that another employee was notified of an irregularity. It did not take long to discover the fraud, and Lewis was convicted of embezzlement. He was sentenced to five years in a federal prison.

Since Lewis was obliged to be physically present to trap the fraudulent check as they came through the system, he could not afford to have anyone with him watching what he did. I doubt that Lewis would have been enthusiastic about having to train a backup to do his job. If anyone had been

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

cross-trained, I doubt the embezzlement would have continued so long and been so serious.

Another even more sensitive topic is vacation time.

Lloyd Benjamin Lewis took his unauthorized duties (stealing money from his bank) so seriously that during the entire period of his embezzlement, about 850 days, he was never late, never absent, and never took a single vacation day in over two years. As a data center manager, I would have been quite alarmed at having an employee who had failed to be absent or late a single day in more than two years. How would you know what would happen if Mr Perfect really were away? The usual rule in companies is that if an employee fails to use vacation days, they can be carried over for a limited time and then they expire. This is supposed to be an incentive to take vacation time. For normal, honest employees it probably works fine. For dishonest employees who have to be present to control a scam, losing vacation days is irrelevant.

I recommend that every employee be required to take scheduled vacations within a definite – and short – time limit. No exceptions should be permitted. Excessive resistance to taking vacations should be investigated to find out why the employee insists on being at work all the time.

The problem is that the devoted, dedicated employee can get caught up in a web of suspicion precisely because of exceptional commitment. The only ways I can think of to avoid difficulties of this kind are (1) to make the reason for the policy well known to all employees so no one feels singled out; (2) to rely on the judgement and discretion and good will of the investigating manager to avoid hurt feelings in their most loyal employees.

### 2.6 Changes in Behavior

Any kind of unusual behavior can pique the curiosity of a manager. Even more important from a security management standpoint, any consistent change in behavior should stimulate interest. Is Miss Punctual suddenly late–day after day? Did Mr Casual start showing up regularly in hand-tailored suits? Why is Miss Charming snarling obscenities at her staff these days? What accounts for Charles' working overtime every day all of a sudden – in the absence of any known special project? Is Yosuf, that paragon of perfection, now producing obvious errors in simple reports? How is it that the formerly complaisant Waclav is now a demanding and bitter complainer?

Any radical change in personality should elicit concern, too. If the normally relaxed head accountant now has beads of sweat on her forehead whenever you discuss the audit trails, perhaps it's time to look into her work more closely. Mr Bubbly is now a morose whisky-swilling sourpuss: why? The formerly grim Schultz now waltzes through the office with a perpetual smile on his face. What happened? Or what is happening?

All of these changes alert you to the possibility of subterranean changes in the lives of your employees. Although these changes do indeed affect the security of your organization, they also concern managers as human beings who can help other human beings. Mood swings, irritability, depression, euphoria–these can be signs of psychological stress. Is your employee becoming alcoholic? a drug addict? abused at home? going through financial difficulties? having trouble with

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

teenagers? falling in love with a colleague? Of course you can't help everyone, but at least you can express your concern and support in a sensitive and gentle way. Such discussions should take place in private and without alarming the subject or exciting other employees. If you feel out of your depth, by all means involve your human resources or personnel department. They will either have a psychologist or trained counselor on staff or be able to provide appropriate help in some other way such as an Employee Crisis Line.

There are sad cases in which employees have shown signs of stress but been ignored, with disastrous consequences: suicides, murders, theft, and sabotage. Be alert to the indicators and take action quickly.

With so much of our organizations' financial affairs controlled by information systems, it is not surprising that sudden wealth may be a clue that someone is committing a computer crime. A participant in the Information Systems Security Course reported that an accounting clerk at a U.S. government agency in Washington, D.C. was arrested for massive embezzlement. The tipoff? He arrived at work one day in a Porsche sports car and boasted of the expensive real estate he was buying in a wealthy area of the Capital region.

Not all thieves are that stupid. A healthy curiosity is perfectly justified if you see an employee sporting unusually expensive clothes, driving a sleek car after years with a rust-bucket, and chatting pleasantly about the latest trip to Acapulco when their salary doesn't appear to explain such expenditures. On the other hand, being a nosy Parker who butts into people's private lives will win you no friends. It's a real bind but ignoring the issue doesn't make it disappear.

The other kind of change – towards the negative – may also indicate trouble. Why is your system manager looking both dejected and threadbare these days? Is he in the throes of a personal debt crisis? in the grip of a blackmailer? beset with a family medical emergency? a compulsive gambler on a losing streak? Again, on humane grounds alone you would want to know what's up in order to help. As a manager concerned with security, you have to investigate. In these days of explosive rage and ready access to weapons, ignoring employees with a dark cloud hovering over their heads may even be irresponsible and dangerous.

The manager's job is a tough one: you must walk the thin line between laissez-faire uninvolvement (and risk lifelong regrets or even prosecution for dereliction of duty) and overt interference in the private affairs of your staff (and risk embarrassment and prosecution for harassment).

Written policies will help you; so will a strong and ongoing working relationship with your human resources staff. Making it clear to all employees that managers are available for support and expected to investigate unusual behavior will also help avoid misunderstandings.

## 2.7 Separation of duties

The same principles that apply to the control of money should apply to control of data. Watch the tellers at a bank: when you deposit a large check, you'll see the teller going to a supervisor and having that person look the check over and initial the transaction. When bank tellers empty the

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

automatic teller machines at night and fill the cash hoppers, there are always two people present. The person who creates a check is not the person who signs it.

In well-run information systems departments, data entry is distinct from validation and verification. For example, a data entry supervisor can check on the accuracy of data entry but cannot enter a new transaction without having their direct supervisor check their work. There is no excuse for allowing the supervisor to enter a transaction and then, effectively, authorize it. What if the entry were in error – or fraudulent? Where would the control be?

In quality assurance for program development, the principles of separation of duty are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. Test systems are separate from production systems; programmers must not have access to confidential and critical data which are controlled by the production staff. Programmers must not enter the computer room if they have no authorized business there; operators must not modify production programs and batch jobs without authorization.

When I ran operations at a service bureau many years ago, I trained two systems managers as soon as I could to take over the day-to-day management of the computer systems. When they were ready, I asked them to remove system manager capabilities from my account. I had no wish to intrude on their province of responsibility. My meddling with system parameters would cause more trouble than it would solve. Were there to be an emergency, I could be granted system management permissions and resume my former role. This attitude exemplifies the concept of separation of duties.

In early 1995, the financial world was rocked by the collapse of the Barings PLC investment banking firm. The Singapore office chief, Nicholas Leeson, was accused of having played the futures market with disastrous consequences. The significant point in our context is that he managed to carry out all the orders without independent overview. Had there been effective separation of duties, the collapse would not have occurred.

A related approach is called dual control. As an example of dual control, consider the perennial problem of having secret passwords not know to management yet sometimes needing emergency access to those passwords. This problem does not generally apply to ordinary users' passwords, which can normally be reset by a security administrator without having to know the old password (and which are then changed to a truly secret string by the user after a single logon). However, if there is only one person who has the root password for a system (say, because the other system manager is on vacation) then it makes sense to store a written copy of the root password in a truly opaque envelope, seal it, sign the seal, tape over the seal with non-removable tape, and then store the envelope in a corporate safe. The principle of dual control dictates that such a copy of the root password should be accessible only if two officers of the organization simultaneously sign for it when taking it out of the corporate safe.

In conclusion, think about the structure of control over information as you design your INFOSEC policies and make sure you are providing separation of duties or dual control throughout your systems.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

# 3 FIRINGS AND RESIGNATIONS

I started this article with hiring; the other end of the employer employee relationship also deserves attention from a security conscious manager. Taking our security mandate in the widest sense, we have to protect our employer and ourselves against potential damage from unethical, disgruntled or incompetent employees and against the legal consequences of improper firing procedures. Common sense and common decency argue for humane and sensitive treatment of people being fired and those who are resigning.

## 3.1 Resignations

The potentially most dangerous form of employment termination is the resignation. The problem is summed up in the caption of a cartoon I once saw. A savage attack is in progress against a medieval town; a clan war chieftain confronts a singed and dirty warrior. "No, no, Thor! Pillage, THEN burn!" Like the warriors, employees rarely resign without planning. An employee may have an indefinite period during which he or she knows that resignation is imminent, whereas the employer may remain unaware of the situation. If the employee has bad feelings towards or evil designs on the current employer, there is a period of vulnerability unknown to management. Dishonest or unbalanced employees could steal information or equipment, cause immediate or delayed damage using programmatic techniques (the so called "logic bomb"), or introduce faulty data into the system ("data diddling").

The policies discussed in previous articles for ongoing management should reduce the risks associated with resignations. Your goal as a manager should be to make resignations rare and reasonable. By staying in touch with your employees' feelings, moods and morale, you can identify sources of strain and perhaps resolve problems before they lead to resignations and their associated security risks.

## 3.2 Firings

Firings give the advantage to employers. The time of notification can be controlled to minimize its effects on the organization and its business. For example, employers might find it best to fire an incompetent or no longer acceptable employee before beginning an important new project or after a particular project has finished.

Some people argue that to reduce the psychological impact on other employees, they fire people at the end of the day, perhaps even before a long weekend. The theory is that the practice gives everyone a cooling off period outside working hours. These managers say they don't want the buzz of conversation and speculation that often follow a firing to intrude on the work day. This policy fails to regard the psychological stress to employees who have a ruined weekend and no way of responding constructively to their potentially catastrophic loss of a regular income.

A better approach to this stressful task is to fire people early on Monday morning in order to provide an unrushed exit interview and job counseling to help the employee prepare for job hunting. In this scenario, the regrettable necessity (from the manager's point of view) of terminating employment is buffered by professionals in the human resources department who can give the

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

departing employee a sense of hope and some practical as well as emotional support in their difficult time. This humane attitude is particularly important when there are many people being fired – one of the worst experiences possible for both employees and managers and an event that has serious security implications.

### 3.3 Doing it wrong

A participant in one of my courses told the following horrifying tale of a firing gone wrong: in a large company, the personnel department asked information security staff to suspend the access codes for more than 100 people who were to be fired at 18:00 on Tuesday. On Wednesday at 08:00, the security staff began receiving phone calls asking why the callers' logon IDs no longer worked. It turned out that the personnel staff had failed to inform the "victims" on time. The psychological trauma to both the employees who were fired and to the security staff was severe. Several security staff members were sent home in tears to recuperate from their trauma. The harm done to the fired employees was even more serious, and the effect on morale of the remaining employees was a disaster. It's a wonder that there was no violence in that situation.

### 3.4 Cross-training again

One of the key organizational issues in planning or responding to termination of employment is training replacements for the departing employee. Such needs are voiced to justify policies allowing a more graceful, civilized and friendly approach to firings and resignations. It seems reasonable to encourage the departing employee to train the colleagues or new employees who will assume his or her responsibilities. However, cross training should be part of the normal operations of all organizations.

In conclusion, firing people is a stressful time for everyone concerned and leads to increased security risks. Managers should do everything in their power to ensure a courteous, respectful and supportive experience when terminating employment.

### 3.5 How to Say Goodbye

Let's suppose the time has arrived for an employee and the employer to part company. In both resignations and firings, security consultants unanimously advise instant action. Not for them the leisurely grace period during which employees wind down their projects or hand them off to other staff members. No, security officers are a hard lot, and they advise the following scenario: in a formal exit interview, and in the presence of at least two managers, an officer of the employer informs the employee politely that his/her employment is at an end. During the exit interview, the officer explains the reasons for termination of employment. The officer gives the employee a check for the period of notification required by law or by contract (e.g., this could be at least the same period as that between pay checks) plus any severance pay due. Under supervision (preferably in the presence of at least one security guard), the employee is escorted to their work area and invited to remove all personal belongings and place them in a container provided by the employer. The employee returns all company badges, IDs, business cards available, credit cards, and keys. The employee is then ushered politely outside the building.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

At the same time as all this is happening, all security arrangements must be changed to exclude the ex employee from access to the building and to all information systems. Such restrictions can include:

- striking the person's name from all security post lists of authorized access;
- explicitly informing guards that the ex employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- changing the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;
- removing or changing all personal access codes known to have been used by the ex employee on all secured computer systems (microcomputers, networks, mainframes);
- informing all outside agencies (e.g., tape storage facilities, publications with company advertising) that the ex employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;
- requesting cooperation from outside agencies in informing the employer if ex employees attempt to exercise unauthorized functions on behalf of their former employer.

The task is made more difficult by seniority or if the ex employee played an important role in disaster recovery or security. The employer should be assiduous in searching out all possible avenues of entry resulting from the person's position of responsibility and familiarity with security procedures.

In one story circulating in the security literature, an employee was fired without the safeguards suggested above. He returned to the workplace the next Saturday with his station wagon and greeted the security guard with the usual friendliness and confidence. The guard, who had known him for years, was unaware that the man had been fired. The ex employee still had access codes and copies of keys to secure areas. He entered the unattended computer room, destroyed all the files on the system, and then opened the tape vault. He engaged the guard's help in loading all the company's backup tapes into his station wagon. The thief even complained about how he had to work on weekends. This criminal then tried to extort money from the company by threatening to destroy the backup tapes, but he was found by police and arrested in time to prevent a disaster for his ex employer.

### 3.6 Psychosocial Issues in Firing People

In this series, we are reviewing some of the implications of personnel management for information security. In several previous articles, I discussed practical considerations in how to terminate

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

employment with the least possible suffering and the lowest threat to security. In this article, I want to look at the social and psychological effects of employment termination in a bit more detail.

What, no farewell party? Alas, security does interfere with the more obvious signs of friendliness. The problem with a farewell party is that there may be litigation if employees leaving under a cloud feel humiliated when most people get a party but they don't. Generally it makes sense to treat all departing employees the same if the termination is involuntary.

However, nothing stops a humane and sensitive employer from encouraging employees to arrange an after hours party even for people who have been fired.

On the other hand, if a resignation is on good terms, the employer may even arrange a celebration, possibly during working hours and maybe even at company cost.

A firing or a resignation on poor terms has two psychological dangers: effects on the individual concerned (embarrassment, shame, anger) and effects on the remaining staff (rumors, resentment, fear).

Both kinds of problems can be minimized by publishing termination procedures in organization documents provided to all employees; requiring all employees to sign a statement confirming that they have read and agreed to the termination procedures; and consistent application of the termination procedures.

The personal shock of being fired can be reduced by politeness and consideration consistent with the nature of the reasons for being fired – although even nasty people should not be subject to verbal or physical abuse no matter how bad their behavior; treatment consistent with that meted out to other fired employees; and generous severance arrangements.

I once had to leave a wonderful company because of reasons beyond the control of the employer and myself. Neither the company nor I wanted to terminate my employment. The owner of the company offered to continue paying my salary until I found a job – and urged me to take all the time necessary to find a satisfactory job. His generosity eased the shock of having to leave my friends and colleagues.

Organizational turmoil can be reduced by convening organization wide or departmental meetings to brief remaining employees on the details of significant termination; open discussion, including understanding how people respond to rupture of relationships. The remaining employees may have to suffer grief (a process, not a state).

Grief is a normal and healthy response to disruption of relationships (e.g., death of a loved one, divorce, and even the loss of a co worker). Some people value social relationships more than other aspects of their work and may be especially affected by firings. Grief involves stages of denial, anger, mourning and recovery. Trying to forestall such responses by denying that people legitimately have feelings is foolish and counter productive. It is far better to encourage those who are upset to voice their feelings and to engage in constructive discussion than to clamp down pointlessly in a futile attempt to suppress discussion.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

### 3.7 Style

The way an organization handles job termination affects more than internal relations. It also influences its image in the outside world. Prospective employees will think twice about accepting job offers from an organization that maltreats departing employees. Clients may form a negative impression of a company's stability if it abuses its own people. Investors may also look askance at a firm that gets a reputation for shoddy treatment of employees. Bad employee management relations are a warning signs of long term difficulties.

Finally, just in case you are wondering if this is still a security column, yes indeed! All of the factors mentioned above affect the foundation for sound information security. People are the key to effective INFOSEC, and disaffected employees and angry ex-employees are still important threats according to many current studies. For example, the annual computer crime survey published by the Computer Security Institute in March 2000 (see < http://www.gocsi.com/prelea_000321.htm > ) suggested that computer crime threats to large corporations and government agencies come from both inside and outside their electronic perimeters, confirming the trend in previous years. Seventy one percent of 643 respondents detected unauthorized access by insiders.

### 3.8 Legal issues in firing people

There's another dimension to employment termination that depends on local laws and the litigation environment. The United States, for example, is said to be one of the most litigious nations on the planet, perhaps because of the high number of lawyers per capita.

Now, let's be sure everyone understands the obligatory disclaimer to avoid going to jail for dispensing legal advice without a license: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney.

However, simple experience does teach one some principles even without going to law school. Here are some pragmatic guidelines for preventing legal problems related to firings:

- Build a solid, documented case for firing someone before acting. Keep good records, be objective, and get the opinions of several trustworthy people on record.
- Give the employee clear feedback long before considering firing.
- Offer the delinquent employee all reasonable chances to correct his or her behavior.

Timing is important in employee relations, as it is in almost everything else we do. In particular, if an employee is found to be behaving improperly or illegally, there must be no marked delay in dealing the with problem. Such a person could sue the employer and individual managers. They could argue in court that the very fact that there was a delay in firing them was proof that the firing was due to other factors such as personality conflicts, racism, or sexism. A well defined procedure for progressing through the decision will minimize such problems.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.* 

The critical legal issue is consistency. If rules such as those described above for the day of the firing are applied haphazardly, there could easily be grounds for complaining of unfairness. Those to whom the rules were strictly applied would justifiably feel implicitly criticized. How would we feel if we were singled out by having guards check what we took home from our desk – if everyone else got a party and two weeks notice? Such inconsistency would be grounds for legal proceedings for defamation of character. The company might lose and it might win, but what non lawyer wants to spend time in court?

Another issue that arises in connection with firings and resignations is non-disclosure agreements. All such agreements must be included in a contract signed before the prospective employee begins work; it is impossible to force an existing employee to sign such an agreement. I remember one employer approaching me two years into my contract with them and asking that I agree that all patents I might develop – even those resulting from work at home in off-hours–would belong to the employer. I refused, and there was nothing they could do about it (well, fire me, maybe). Any attempt to threaten an employee with dismissal could result in a successful lawsuit for breach of contract and, if the threat were carried out, wrongful dismissal.

You, your legal department and your personnel department should study the necessity and feasibility of instituting a legally-binding contractual obligation to protect your company's confidential information for a specified period of time after leaving your employ. You cannot impose indefinite gags on people, but one year seems to be normal. For this measure to be meaningful, you must include a clause in the initial employment contract that requires the departing employee to reveal his new employer, if there is one at that time.

Non-competition agreements require the employee to refrain from working for direct competitors for perhaps a year after termination of employment. The key to a successful clause here is that there be a strict, operational definition of "direct competitors." Because this limitation can be an onerous impediment to earning a living, many jurisdictions will forbid such clauses.

*Copyright ©2000, 2006 M. E. Kabay. All rights reserved.*