

# Employment Practices & Policies

by M. E. Kabay, PhD, CISSP-ISSMP  
Professor of Computer Information Systems  
School of Business & Management  
Norwich University, Northfield VT

Because people execute security policies (or violate them), hiring, managing and (alas) firing are important aspects of information assurance (IA) management. In a recent class discussion of personnel policies and security, the IS342 Management of Information Assurance <<http://www.mekabay.com/courses/academic/norwich/is342/index.htm>> class reviewed some of the fundamental principles of personnel and security.

To start with, we face two fundamental problems in all discussions of crime, especially white-collar crime, and particularly computer crime: we have incomplete ascertainment and we have incomplete reporting.

The problem of ascertainment lies in the difficulty of identifying crimes or errors that compromise confidentiality and control, at least until the malefactors reveal the data leakage by using the purloined information. And unfortunately, we don't yet have any centralized reporting of computer crimes or legal requirements for contributions to such a central database – so we lack reliable estimates of the frequency and severity of computer security breaches.

Nonetheless, a broad consensus among IA practitioners does support the belief that a sizable proportion of damage to computer systems may be from errors and omissions – perhaps even half. The attacks from the outside of systems and networks have increased over the last two decades because of the huge increase in interconnectivity due to wide use of the Internet.

Under these conditions, selecting appropriate employees can be a major contribution to effective IA. This review looks at hiring, management and firing from the perspective of IA managers.

## Hiring

Everyone with access to organizational information must be trustworthy; furthermore, it makes sense to put extra care into the hiring process for all employees who will be supporting computer systems such as operators, technical support personnel, programmers, managers, and security officers.

A degree of background checking is appropriate, but must respect applicable laws against discrimination in hiring. With the permission of the candidate, one can look for criminal records, and credit records as well as verifying claims of educational attainment and professional experience. Don't expect former employers to reveal much detail about the candidate beyond the dates of her employment; organizations are now highly sensitive to the risk of violating privacy laws or of stumbling into lawsuits for defamation.

In my experience as a technical services director for a sizable computer services company

several decades ago, I found it particularly helpful to have candidates for a particular job be interviewed by the staff currently involved in that kind of work. The staff can gently probe the candidates' bona fides with more detailed knowledge of the work that will be required than a manager who is some remove from the day-to-day details of a job. They can also spot frauds more easily through their questioning; I remember one case where a poor fellow claimed to have three years of experience on the HP3000 (a "minicomputer" – think a big server) popular in the 1980s yet who could not log on to the system!

During the hiring process, successful candidates must be thoroughly briefed on corporate policies such as non-disclosure agreements for intellectual property, compliance with all regulations, and penalties for non-compliance. Some organizations have found it helpful to have a simple examination (usually automated) for the candidate to demonstrate knowledge of applicable policies.

## **Management**

One of the key attributes of successful security officers is the ability to assume an attitude of paranoia. You don't have to be paranoid: you just have to be able to act paranoid. Analysing how employees might abuse security systems and regulations is a constructive exercise in critical thinking. Security teams can benefit from exercises in thinking through how abuses could be carried out, how to respond, and how to improve processes to reduce risk. The organization should foster a belief in continuous process improvement, with suggestions for improvement welcomed, not criticized, and perhaps even rewarded. In one of my client sites, a factory, I remember seeing a poster that showed one of the employees with a big check – literally big: it was a couple of feet wide – made out for C\$25,000. That amount (even more impressive than today in 1983) was 10% of the savings the employee had fostered in the first year through a suggestion for modifications in the production environment.

Another critical tool in training employees is how to respond to attempted collusion. An employee can practice dealing with such an uncomfortable situation in training sessions to get used to the idea that the first response should be to appear interested; the second is to report the attempted collusion to management so they can decide on appropriate actions (e.g., create a sting operation, record interactions with the criminal, and contact law enforcement).

One of the principles I teach is that access to computer systems or information is a privilege, not a right. It is unwise to grant access privileges to managers who don't need it – there's a risk that access will become a status symbol instead of a privilege tied to specific job requirements. One of the incidents that I recall with amusement occurred around 1985 when the president of the company I worked for brought a visitor from Toronto to our Montreal data centre on a Saturday night and asked the operator to let them into the computer operations room. The operator politely refused because the president was not on the list of approved unaccompanied visitors. The young man offered to call me for permission, but the president took the snub in good spirits. Indeed, he wrote a letter of commendation for the operator a couple of days later.

Another principle is "Kabay's Law:" NO ONE SHALL BE THE SOLE REPOSITORY OF CRITICAL INFORMATION OR SKILLS. There was a horrible example of the consequences of violating this principle in a case I was involved in the mid-1990s. A network administrator for the three offices of a law firm was increasingly erratic in his behaviour – and we consultants had

to meet offsite because there was reason to believe that he was reading all the e-mail of the executives! He was the only person who knew the root-access password, and he had never documented it in a way that his colleagues could have accessed. Dealing with an indispensable employee can be difficult. The norm must be that all operationally significant information must be documented; appropriate security for such documentation can include sealing passwords into opaque envelopes stored in the organization's safe and accessible when two high-placed executives sign for it. Periodic testing of such repositories is appropriate.

On the procedural side, everything that affects the mission-critical operations of the organization must be part of the institutional knowledge of the group. At least two people should always be able to accomplish any given critical task; they don't have to be perfect at it, but the disappearance of the prime should not put the organization in jeopardy.

Another guide for managers is to enforce vacations. There are two reasons for insisting on vacations. First, vacations offer an opportunity for live testing of the principles of operational resilience described above. Second, vacations offer an opportunity to see if someone has been carrying out secret operations that must be continued to avoid discovery. For example, if an accountant has been embezzling money by paying fake companies for non-existent services or goods (and using the fake bank accounts for his own benefit), a two-week absence may reveal the crime when another employee notices the fake entries and investigates what they were supposedly for.

If employees change their interpersonal style radically – whether for good or ill – supervisors might want to look into the situation. Becoming friendly (or angry, or depressed) does not mean necessarily that an employee is involved in anything bad, but managers will do well to investigate. I remember one astounding case where a modestly paid employee showed up at work with an expensive new car and claimed he had won a lottery. However, there was no public record of his winning anything – but investigation of his work showed that he was involved in taking bribes for relaying sensitive information.

The principle of separation of duties means that no critical operation should be completed by a single person. In the embezzlement scenario, it was a problem that the accountant was able to create invoices, approve them, and pay them without supervision.

Another warning for employers is that security policies must absolutely forbid unauthorized security testing. There have been many cases in which well-meaning employees have been fired for foolishly testing system security without informing anyone in advance and obtaining written authorization by a suitable manager. And on the converse side, claiming good intentions for security probes may be a cover for nefarious plans.

## **Termination of Employment**

Well, things haven't gone as well as they should. One or more employees must be fired for reasons such as workforce reductions, mergers and acquisitions, or inadequate individual performance. The basic rule is that absolutely everyone must be treated with the same procedure and the same respect, regardless of manager's emotions about the termination. If Albert is frog-marched to the exit by a security guard whereas Betty is treated to a joyful party, the message is clear: Albert is bad and Betty is good. Such implicit criticism and praise can lead to lawsuits for defamation (by the Alberts). It is best to maintain strict even-handedness when firing people;

then the employees can organize a farewell party privately, on their own time, off the organization's premises.

What about resignations? What is old Charlie has worked diligently for 30 years and is beloved by all? Can't we have a farewell party on the organization's premises? Well, it's a pity, but in a litigious environment, it's best to have the party off premises. Now, Charlie probably let people know about his pending resignation months or years before the event (for example, I have already told my Dean to expect my resignation at the end of May 2025), so there is no need for any surprise in how he is treated. Furthermore, it may be valuable for Charlie to help document details of his work that may not have made it into institutional knowledge and to train his replacements. Nonetheless, exactly the same process as for anyone else would apply to Charlie on the last day of work – the exit interview, clearing the desk, returning identification cards, and returning other corporate property.

An exit interview can be either a painful exercise or a positive experience. If the separation is amicable, the departing employee may be able to contribute insights that might have been more difficult to impart to managers while she was employed. Even if there is some friction underlying the departure, it's still possible to extract useful information from the employee if she is willing to speak her mind.

Finally, the termination process must be tightly coordinated between the human resources group and the information technology and IA group. As the exit interview is underway, the employee's access privileges must all be revoked and assigned to appropriate replacement personnel who will take up the tasks of their former colleague.

For a more detailed version of these points, you can see Chapter 45, "Employment Practices & Policies" by myself and Bridgett Robertson in the *Computer Security Handbook*, 5<sup>th</sup> edition.< <http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/> >. For a PowerPoint presentation on the subject, you can freely download a PPTX< [http://www.mekabay.com/courses/academic/norwich/is342/is342\\_lectures/csh5\\_ch45\\_employment\\_practices\\_policies.pptx](http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch45_employment_practices_policies.pptx) > file or a PDF< [http://www.mekabay.com/courses/academic/norwich/is342/is342\\_lectures/csh5\\_ch45\\_employment\\_practices\\_policies.pdf](http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch45_employment_practices_policies.pdf) > version of the lecture notes.

\* \* \*

M. E. Kabay,< <mailto:mekabay@gmail.com> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< <http://www.mekabay.com/> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.