Managing Your Information Systems:

Training and Security

by Christian Burger & Laurence True

In previous articles, we discussed different aspects of systems acquisition, implementation, and maintenance. This leaves training and security, the two most important (and often overlooked) functions, for last. Both require careful assessment *before* proceeding with major changes to the way you currently manage your systems. Here are some guidelines you can use in planning for training and security.

Training

Construction firms wouldn't dream of letting workers onto a jobsite without first being trained on the heavy equipment they will operate! Yet, we frequently see companies with large investments in hardware and software allowing people to work inefficiently due to lack of training. From the moment new systems are installed, ongoing training is a must. People first need to learn the new system; then, they need updates, refresher courses, and new tips and tricks to continue making the most efficient and effective use of their computer tools. Two caveats, however: Not all training is the same, and different levels of training are needed to get the most out of your information systems investment.

Training Key Players

Many of the systems sold today are *tailorable (*i.e., screen layouts, field names, workflow, even business rules may be changed or customized), thus providing an extraordinary amount of user flexibility. In order to take advantage of this attribute, a user (or, preferably, several users) must gain expertise in how the system works. This requires a higher level of training than typical users will be receiving, and explains why tailorable systems take longer and cost more to implement.

The people who receive this "expert" training will be your *super users*, so select these individuals carefully. They will play an extensive role in the reengineering of your company's business practices and, ultimately, in the training of your end users. A classroom at the software developer's office is the best place to hold this in-depth, highly technical training.

End users, trained after the system is installed, tested, and ready to go live, will receive only a fraction of the training the super users receive, since their use of the system is limited to functions specific to their jobs. This training is best provided in-house where people have access to their own data.

Training your *systems administrator* is as important as training your users. This key person must learn a number of new functions, depending on what is changing as a result of the new system. Systems administrators are not always concerned about applications; however, they must know the hardware and operating system in order to tune the system for performance, as well as perform proper backups.

They may also need some specific training from the company that developed the database used by the software you have chosen. For example, Oracle, IBM, and Microsoft all provide specific training on their products that goes beyond that provided by the application developer.

Other Training

Depending on your company's size and systems complexity, one or two users may also be trained on such functions as report writing, data warehouse creation, and interfacing with your Web site or other software. And, if you use word processing or human resources software, ensure that your people are properly trained on these applications also. Don't assume they'll just "pick it up" from using the system! Users should not be expected to learn new systems or procedures by osmosis. However, not all third-party training programs are adequate, so be careful to check references before using outside training sources.

Report writers (e.g., Crystal Reports, Business Objects) are wonderful tools, and most construction companies benefit from having one of them available. However, they can be a "black hole" for the truly creative talents in your organization. You don't want project managers spending hours finessing your report-writer program just to get a job cost report to look a particular way. Report-writer and database training for one or two systems people, though, could enhance your company's overall satisfaction with its system by enabling your people to create some of the reports they truly need.

Here are a few quick training do's and don'ts:

- *Don't skimp.* Theoretically, you probably can do too much training, but most companies aren't at risk yet.
- *Do allow trainees the opportunity to focus on learning.* Make sure they are able to step away from their daily jobs when they train. Constant interruptions are not fair to the trainee or trainer, and also suggest that management does not view the training as important.
- *Don't train too far in advance.* Ideally, your users should come back from training and immediately begin applying what they have learned. If too much time passes between training and systems implementation, their knowledge will fade.
- *Do build the training in a logical order.* Make sure your trainees understand the basics before moving on to more advanced areas. Otherwise, they will spend considerable time lost and confused during the advanced training, and ultimately become frustrated.
- *Don't assume a strong systems user will make a good trainer.* In fact, some of the best systems users have little patience for slower learners or "technophobes." Training users is about making people comfortable with their new tools and skills, not about how fast the trainer can transfer his or her knowledge. Effective training requires empathy and patience, in addition to systems knowledge.
- *Do gauge the audience.* Your trainer must be alert throughout the training sessions for signs of receptivity and understanding among the audience. Direction and speed must be continually adjusted based on the audience's performance. The goal is not just to get through the text book, but to meet the needs of those being trained.

One Final Word about Training

As mentioned earlier, ongoing training is important. For instance, refresher courses are helpful when new updates are received. On the other hand, tips and tricks can be passed along, a few at a time, simply by having a super user provide one or two new ideas each month during a short, informal breakfast or lunch meeting. This approach will not overwhelm end users, and will also make it easy for super users to develop ideas or materials. Blending learning into a social environment usually goes over well.

Remember, if you are ever in doubt about the value of training or need to convince someone else of its value, just evoke the picture of a large jobsite with lots of heavy equipment and untrained operators. You shouldn't need to say much more!

Security

Door locks, it is said, are intended to keep out honest people. The same can be said for computer security; it will not stop the serious hackers with enough time on their hands. So, in that respect, security is an area that should be given *appropriate* attention, neither too little nor too much.

But, like everything else in technology today, the issue of security is no longer simple. And, given the amount of information most companies now store electronically, the security of that information is more important than ever. The old adage, "An ounce of prevention is worth a pound of cure," is very apropos in this case.

In order to develop an adequate security system, you need to ask, "What are we trying to secure and from whom are we trying to secure it?" Unwanted access to company information is the obvious answer to the first part of that question. And, most people think the obvious answer to the second part is external invaders from the Internet. We'll address external security issues shortly; however, keep in mind that there are so many Web sites on the Internet now that the chance of your site getting hit is remote, and getting more so.

The bigger security threat is internal (including employees and business associates), and ranges from people wanting to hurt your business to prying eyes that simply want to see what somebody else earns. And, surprisingly, some of the most common internal security problems stem from simple things: sharing passwords, leaving unattended computers logged on, and leaving sensitive documents in the printer or on a desk where anyone can read them.

Internal Security

There are three levels of internal security: system, application, and database. Almost everybody does a fairly good job of providing security at the ***system level***. Despite the occasional careless choice of master passwords (such as "master" or "root"), most systems are generally impenetrable to amateurs when properly password-protected. Good rules of thumb about system passwords include not sharing passwords and periodically requiring users to change passwords. It's also wise to require both letters and numbers, as well as case-sensitive passwords, and to avoid using names that could easily be guessed, such as spouses, children, pets, etc.

Many companies fall into the trap of relying on ***application-level*** security to protect their systems. That's a mistake you don't want to make. At this level, security is primarily aimed at ease of use and day-to-day operational control. In reality, application-level security is only effective for preventing ordinary users from roaming around your system at will, looking for information they should not see.

Applications usually provide security at the *menu* and *function* levels, and sometimes at the *specific-record* level. By using these various levels of security, you can prevent certain users from accessing specific jobs, employees, or peripheral equipment, unless they are authorized to do so. But, since application passwords are generally stored in a table somewhere in the system, anyone with a little time can open the table file and find all the passwords.

This is particularly true for popular systems that use a third-party database, such as Oracle, Informix, SQL Server, Btrieve, Progress, DB2, or any of a hundred other ODBC-compliant databases.

Open **D**ata**B**ase **C**onnectivity, a standard database access method developed by Microsoft, makes it possible to access any data from any application regardless of which database management system is handling the data. It also makes it possible for any hacker, armed with a good report writer or query tool, to find and view password (and other) files, unless they are separately protected or encrypted. (More on this later.)

Also, the most elaborate security at the application level does not provide protection at the database level, because most systems today use a relational database with named tables and fields that are separate from the applications. Report-writing tools like Crystal Reports and Microsoft Access provide easy access to data for anybody with a little knowledge of database structure and the time to make a few intuitive guesses.

Remember, looking for files with names such as "pr_master" or "sys_pswd" doesn't take much creativity. Unless database-level security has been put in place or *all* report-writing tools on the system are prohibited in some way from viewing these files, you are providing the keys to your system to anyone with access to a report writer.

Which brings us to the third level of security, the ***database-level***. In some systems, the database or data files can be placed in a secured area, so you can rely on security at the system level to prevent unwanted access to the files. This prevents anyone from accessing data other than through the application software. However, you must know how to do this properly or your system will not work correctly. For example, if you secure a particular file needed by a program, a user may not be able to execute the program properly because the database security makes the needed data "invisible" to that user.

Some databases also have built-in security systems that can be invoked independently of the application programs, thereby, greatly reducing your security worries. These systems prevent access to the data no matter what tools are used – so, report writers could not be used to circumvent security.

Other Security Issues

PC-level programs on workstations that have client-access privileges to the data on a server are another source of security problems. So, if your applications execute on your PCs and your data is stored in a relational database on a server, you could have security problems. Any user with a PC-level programming tool or report writer can access the data on the server unless security is established at the database level on the server. Thus, you must protect against this avenue of access.

One more note about security is in order here. There are many more people today who have knowledge of Windows 95/98 and NT than of Unix, Linux, and OS/400. Thus, there are potentially more hackers who could find a way into such systems. Also, while the security is better, it is not foolproof. Protection at the system level means no one gets in without a valid password. The biggest problem we see with this type of security is that companies don't use it properly.

Many systems administrators don't learn how to properly secure servers or directories from hackers. Most of your users have passwords that provide limited access. They can only update files in common areas, but can't delete files or change the security on files. This security is vital for the protection of mission-critical systems and very sensitive data. It is important that only a few people in your organization know how your security is set up and what the passwords are.

External Security

That covers security from within, but what about security from remote-user access and over the Internet? Two methods commonly used when dealing with the Internet are *firewalls* and *encryption*. A firewall is intended to prevent unauthorized access into your system from outside intruders. Firewalls can be as "thick" as you want them to be, and can also perform tasks such as scanning e-mail for viruses. Companies with Web sites that are updated automatically from the company database use firewalls to prevent intruders from backtracking through these updates to enter the database.

Encryption, the most effective way to achieve data security, protects your data during transmission by scrambling it before it is sent and then unscrambling it upon receipt by an approved party. Encryption is often used when you use your credit card to purchase items via the Internet. (Be aware, though, that not all Web sites use encryption. Secure sites will display *https* at the start of their Web address on the ordering screen, instead of the familiar *http*.)

Virus Protection

Unfortunately, protection from viruses is another kind of security that you must worry about these days. Viruses are increasingly common and can be transmitted in several different ways. The newest ones ride in on a *cookie* (a piece of data transmitted from a Web site to a visitor's server), then wait for an opportune moment to open and unleash their damage. So, be very careful when receiving data from unknown sources.

Virus-protection software is a must for most servers and workstations. It is important, however, to update that software regularly from the provider's Web site or through an update service. McAffee and Norton are commonly considered the best virus protection software for PCs and Windows NT servers.

These companies are developing new "antibodies" and detection files almost as quickly as the non-productive members of society can create new viruses. One of the main attractions of Linux for use in servers and firewalls is that the viruses that attack Windows-based machines cannot attack Linux.

And, don't assume that because your primary file servers have virus protection, individual workstations don't need it, as well. All workstations should have virus-protection software; users need it to run a scan-disk program on their hard drive (manually, if necessary) and to scan diskettes they receive from outside the company.

Also, don't open e-mails from addresses you do not recognize. You don't need to download a file to expose your system to a virus; just opening the e-mail can do it.

Conclusion

One final note on both training and security: The administration of a good information system is no longer a part-time job. Secure data, secure systems, and a well-trained user community are important to your company's success. Now more than ever, it's crucial that the responsibility for developing and maintaining systems security and training are assigned full time to someone in your organization. If that is not practical, then find a resource outside the company to provide these critically important services. BP

About the Authors

Christian Burger is the President of the Burger Consulting Group located in Chicago, Illinois (e-mail: crb_burger-consulting@msn.com or phone: 630-510-1875). Prior to establishing his own consulting firm, Christian was a management consultant for FMI for eight years and a client manager for J. D. Edwards for one year.

Christian received his BS in Accounting from Ball State University and is currently working on his MA in Liberal Studies from Northwestern University. He is a member of CFMA's Chicago Chapter and a frequent speaker at industry events across the country.

Laurence True is a Senior Consultant for Burger Consulting Group in Clifton Park, New York (e-mail: larry_c_true @msn.com or phone: 518-373-2865). Prior to joining Burger Consulting Group, he was a Sales Manager and Vice President at Shaker Computer & Management Services.

Larry has more than 30 years experience in systems consulting, implementation services, and information management in the construction industry. Larry, a member of CFMA's Western New York Chapter, holds a BS in Civil Engineering from the University of Colorado, and is a frequent writer and lecturer on computer-related topics.