You Don't Trust me Anymore!

by Carol Woodbury

This may be the cry of your teen-agers as you impose earlier curfews and restrictions on where they can roam. But usually, they've done something to deserve the curbs you're trying to place on their behavior. Unfortunately, the cry I often hear is coming from administrators and programmers as restrictions are being placed on their actions and the functions they are allowed to perform on the system. The difference between these folks and your teen-agers is that they haven't done anything to 'deserve' the restrictions. And that's their complaint – What have I done? I've never stolen from the company and never will. Why are you taking away my ability to perform my job?

The problem is that they are "victims" of the laws and regulations that are forcing organizations to more strictly control access to the system and provide separation of duties. I believe these restrictions are harder to stomach in the iSeries community than elsewhere because most we are such a loyal bunch and totally dedicated to our work; therefore, the thought of placing restrictions on one's job functions or system access is often personally offensive.

I can't blame administrators and programmers for their reaction. However, they need to understand that the changes are not personal and have nothing to do with whether or not the organization trusts the employee. If an organization doesn't trust an employee, I dare say that the employee would be let go! No, this is an issue of the business implementing sound business practices. It's a wise business decision to reduce user access so that they cannot accidentally upload data when they only intended to download a fresh copy of a file into their Excel spreadsheet. Even more common than choosing to implement sound business practices, organizations are imposing more restrictions in order to come into compliance with numerous laws and regulations being imposed on them.

If you find yourself having to defend your organization's actions to administrators or programmers or if you are one of the ones doing the grumbling, the rest of this column should help provide an explanation of why organizations are being forced to make changes. Let's take a look at some of the laws and regulations driving these changes.

Payment Card Industry (PCI) Data Security Standards

The credit card companies have joined together to fight credit card fraud. The Security Standards Council formed by all of the major credit card companies (Visa, MasterCard, American Express, etc) has clearly placed the responsibility of protecting cardholder information into the laps of the merchants storing the information. The PCI released its second version of the data security standard originally created by Visa and MasterCard. These standards document detailed requirements for any system storing cardholder data. Here are some of their requirements affecting administrator and programmer duties.

> Section 6.3.3 of the PCI Data Security Standard states that there must be separation of duties between development/test and production. This means that programmers can no longer have all rights to the production systems. In fact, most auditors don't want programmers accessing production at all. While this is

unrealistic, the fact is that programmer access to production systems must now be tightly controlled.

Section 6.3.7 requires code reviews

Section 6.4 requires that proper change management procedures be followed for both software changes AND system changes including documentation of the impact, management sign-off, testing and back-out procedures. Many development shops have been following change management procedures for a long time, but it's only been recently that administrators have been held to the same standards – that is, documentation of the changes being made, management sign-off and back-out procedures.

Section 7.1 requires that access to cardholder data be restricted to only those users "whose job requires such access." While developers may need to write programs that store or otherwise use cardholder data, they do not have a business justification for seeing "real" cardholder data. The data used by the programmers needs to simulate cardholder data but not be the "real" thing. In fact, Section 6.3.4 specifically states that production data cannot be used on test systems.

Section 8.5.8 states that no accounts or passwords can be shared. I know many administrators that share the password for QSECOFR and other IBM-supplied profiles. A different process will have to be developed for setting and maintaining these passwords. If you and others are currently signing on to QSECOFR to perform tasks, you should be creating individual powerful profiles and using those rather than having several people sign on to the same profile.

Section 8.5.9 states that all passwords must be changed every 90 days. There are a number of Administrators and Programmers who like the password they've used for the last 15 years and don't want to have to think up or remember a new one. That practice has to stop and your new password has to comply with the password rules set on the system. No fair, Administrators, using the Change User Profile (CHGUSRPRF) command to set a new password that is weak and easily guessed!

Health Insurance Portability and Accountability Act (HIPAA)

All of us are aware of HIPAA because of the Privacy statement we have to sign when we go see the doctor. The data security regulations of HIPAA have had some direct affects on IT processes. One of the first requirements in Section 164.306 which addresses the General rules for the Security Standards is to ensure the confidentiality, integrity and availability of the electronic protected health information. This implies that excess capabilities such as *ALLOBJ needs to be removed from users. Accidental outages or modification of data caused by users having too much authority is a violation of this Standard.

Section 164.308 – Security Awareness and Training requires that passwords be changed on a regular basis.
Section 164.312 – Access controls - requires that access to electronic protected health information be restricted to those with a job function that requires the access.

This section also prohibits sharing of passwords and the need to regularly change passwords

Gramm-Leach Bliley Act (GLBA)
Those of you in the finance industry are probably familiar with GLBA. A recent addition to the requirements of GLBA include a security self-assessment questionnaire that must be filled out in its entirety and signed by an executive officer attesting to its validity and accuracy. Inquiries are made as to the change management processes in effect as well as the request to document any known separation or "concentration" of duties issues. In other words, it is no longer acceptable for a programmer to be able to check out a part, change it, test it and promote without someone else reviewing the change and giving the permission for it to occur. Explanations of various aspects of a financial institution's regular auditing and monitoring processes are also required. Questions include whether user access rights are reviewed on a regular basis. You can be assured that more and more scrutiny is being placed on how many and which users have powerful user accounts – or in i5/OS terms, who has *ALLOBJ.

Sarbanes-Oxley Act (SOX)
SOX does not specifically list any data security requirements yet they are heavily implied and some form of data security requirements are required by most SOX auditors. The requirements I see on a consistent basis are for everyone to implement and follow a formal change management process, separation of duties and the documentation of key processes. Building on the intent of SOX, it makes sense that if you are required to ensure the integrity of your financial information, that access to the database files containing the information should be restricted – meaning that you have set *PUBLIC authority appropriately. It also means implementing other security controls to protect the system as a whole. These controls include strong passwords, user profile management (removing excess capabilities, deleting profiles of users no longer with the company, setting system values to the most secure settings where possible and so forth. Intent of SOX is not to stop people from doing their jobs. The intent is to not give users more authority, capability or responsibility than they need or is appropriate for their job function.

Summary
I understand that the changes organizations are making to come into compliance with laws and regulations are often an imposition and cause changes to the way tasks get accomplished. But if you are reading this and you are one of the complainers, please don't take your frustrations out on the messenger (the person implementing the required changes!) If you are the implementer of these changes I hope that you find this list of laws and regulations helpful in explaining to the administrators and programmers why the changes are a matter of compliance; therefore, should not be taken personally. They may still be unhappy about the changes but hopefully they will understand the business compliance issues driving the changes.

Carol Woodbury *is President and co-founder of SkyView Partners, Inc., a firm specializing in security policy and compliance management software as well as security consulting and remediation services. Carol has over 16 years in the security industry, 10 of those working for IBM's Enterprise Server Group as the AS/400 Security Architect and Chief Engineering Manager of Security Technology. Carol's second book, Experts' Guide to OS/400 and i5/OS Security, is available at www.amazon.com .*