SKY VIEW
PARTNERS, LLC

IT Data Security Best Practices

Many Administrators, due to a variety of government regulations in the United States, Canada and other countries, are looking for guidance - or best practices - with IT Data Security. I think that one of the biggest frustrations Administrators face today is not knowing where to start. COBIT, as I discussed, is a framework for assessing, managing and reducing risk associated with IT business practices. But while COBIT provides good guidance, one of the complaints Administrators have with COBIT is that it lacks implementation details. In other words, COBIT doesn't do a good job describing how to implement the methods it describes. Therefore, Administrators are trying to figure out how to determine what security best practices really means and then how to implement them.

This article will describe some places that Administrators can go that describe best practices for IT Data Security as well as how to interpret them.

ISO17799

Many auditors turn to ISO17799 for IT Data Security Best Practices. ISO17799 is based on the British Standard 7799 and outlines implementations for IT Security. ISO17799 addresses the following areas with numerous sub-points for each:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

Unfortunately, to obtain ISO17799 one must purchase it. It's available at http://www.standardsdirect.org/iso17799.htm for about $200.

If ISO17799 is not in your budget, there are some other resources that are available without charge.

Information Security Forum (ISF)

The Information Security Forum (ISF) http://www.isfsecuritystandard.com/index_ie.htm is an international organization made up of 250 organizations that are dedicated to helping businesses protect their critical data and information. Their business practices are documented in The Standard of Good Practice for Information Security (the Standard) which is free to non-members. (Implementation tools are available for a fee.) Their objectives in providing this Standard free of charge are to:

- promote good practice in information security in all organizations

- help organizations improve their level of security and reduce their information risk to an acceptable level
- assist in the development of international standards that are practical, focused on the right areas and effective in reducing information risk.

This standard divides IT Security issues into five aspects:

- System management
- System development
- Business critical applications
- Computer installations
- Network

Though not as thorough as ISO17799, the Standard from ISF does provide a good place to start.

Computer Security Resource Center (CSRC)

The National Institute of Standards and Technology (NIST) has established the CSRC, which also provides some best practices and guidance. This website http://csrc.nist.gov/ is especially helpful if you are in the government sector, are in an industry which requires compliance with FIPS standards or have encryption standards that must be followed.

Gramm-Leach Bliley Act (GLBA) and Health Insurance Portability and Accountabilty Act (HIPAA)

Neither GLBA http://www.ftc.gov/privacy/glbact/index.html nor HIPAA http://www.dhhs.gov/ocr/hipaa/ may be the first place you would think to look for best practices but these acts have some defined some serious data security requirements. Reading the data security portion of these Acts will give you some guidance on what these highly regulated industries require.

Still Frustrated?

As I said earlier, I believe that most Administrators are looking for a place to start. Despite providing this, Administrators may still be frustrated over certain aspects of these best practices documents because they have to take a generic set of “rules” and interpret their meaning for the particular operating system upon which they are working. Unfortunately, that’s the way standards are – specific enough to help you know what’s expected yet generic enough to apply to every operating system. Let’s take a look at some of the issues addressed by ISO17799 and see how one might translate those into OS/400 practices.

Here are some of the details of a couple control objectives addressed within the Access Control section for the User Access Management section:

Control Objective	ISO17799 Wording	OS/400 and i5/OS Interpretation
User registration	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	A formal process should exist for how users get approval for requesting a user profile. When a user leaves the company, a process needs to be in place with HR to delete the profile on a timely basis. If the profile owns objects and you cannot delete the profile right away, at least set the STATUS to *DISABLED.
Privilege management	The allocation and use of privileges shall be restricted and controlled	Special authorities should be given to a user only if they have a job responsibility that requires a special authority to perform. For example, *SECADM special authority should only be given to users than are responsible for creating and managing user profiles.
Review of user access rights	Management shall conduct a formal process at regular intervals to review users' access rights.	Users access to applications as well as what they are able to do within the application needs to be reviewed on a regular basis (no less than one time per year.)
Unattended user equipment	Users shall be required to ensure that unattended equipment is given appropriate protection.	Use the system values QINACJOBITV, QINACTMSGQ, and QDSCJOBITV to time out inactive signed on sessions

If you find yourself needing to interpret what best practices mean in OS/400 and i5/OS security terms, you will need to familiarize yourself with OS/400 and i5/OS security concepts. Recommended reading includes the iSeries Security Reference manual, available from IBM's Info Center www.iseries.ibm.com/infocenter or my new book co-authored with Patrick Botz – Experts' Guide to OS/400 and i5/OS Security. You will also need to familiarize yourself with general security principles and terminology. A good resource for this information is www.searchsecurity.com and their printed magazine, Information Security www.infosecuritymag.com.

Summary

Best practices are a good place to start, especially when putting together a plan to re-architect the security configuration of your system. However the key to a good and workable security implementation is to making it fit your business requirements. One size does not fit all. Best practices, in most cases, have you configuring the system's security settings to the most secure setting. However, there may be times when the most secure setting is too restrictive for your environment. So while many auditors will audit you against best practices, auditors cannot force you to implement the best practices when you can show them the business analysis that says that a certain setting is detrimental to your business.

I encourage you to examine your security configuration settings against best practices and use the best practices whenever possible. When it isn't possible, make sure you have a business risk analysis in place to justify the less secure setting.

Carol Woodbury is co-founder of SkyView Partners, a firm specializing in security consulting and remediation and the assessment product, SkyView Risk Assessor for OS/400 and i5/OS. Carol has over 14 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 can be reached at carol.woodbury@skyviewpartners.com

This information appeared originally in the June 2004 iSeriesExtra Administrator newsletter.