CHAPTER 1

Security—The Reasons You're Reading This Book

When the first version of this book was written by Wayne Madden, the title of this chapter was "Security Is a Business Function." Readers purchased and read the book because they believed in that principle and wanted to learn more. Although that principle is no less significant today, I feel it is important to acknowledge—in the very first chapter—why I believe many of you are reading *this* book.

For many of you, it's because your organization is required to be in compliance with some law or regulation. For others, it's because you've been tasked with implementing a "deny by default" security scheme. Some of you are new security administrators and want to learn the basics of IBM i security. Others may be reading this book because you are auditors assigned to a client running something called an "iSeries" or "IBM i," and you need to understand its security features. Whatever the particular reason, in today's world, implementing a sound security policy is often a forced issue rather than a choice.

So, because you may have picked up this book not so much because you wanted to but because you had no other choice, I've worked hard to make sure reading it will be a good use of your valuable time. To help ensure that it is, I have several goals for this book:

To explain security best practices as they pertain to the IBM i operating system, using clear and understandable terms and concepts. Regardless of the type of

organization to which you belong, in most cases you must comply with some law or regulation. If your organization can implement security best practices, not only will you comply with most current laws and regulations, but you will be in a position to comply with future laws and regulations, or at least not have a difficult time coming into compliance. For this reason, it's important to learn what constitutes security best practices on IBM i.

To give you choices. While I recommend that security best practices be every organization's goal, reality shows that most organizations have some area for which they are unable to implement best practices. This book discusses how to evaluate risks so you can determine which exposures you need to remediate and which you're willing to accept.

To provide practical implementation examples. I've probably seen every range of implementation possible, from the unbelievably open system to the system whose users can barely breathe without permission. Most security implementations lie somewhere in between. This book is full of practical and tested implementations.

To help you gain an understanding of the appropriate security scheme for the organization in which you're working. How am I going to do that? By helping you to identify the type of data being stored on your system and to understand the security implications of maintaining this type of data. Not all systems need to be locked down like Fort Knox. Some systems hold data that can be viewed by all users. Others have data that only a few people should be able to see. Understanding the type of data stored on your system is key to understanding the security requirements you need to apply to that system.

To give you tips for saving time when administering your system. All administrators are pressed for time. I don't want you wasting time discovering for yourself what is important and what can be ignored. I tell you exactly what commands to run to get the information you need—whether the information is required for a report for auditors or you need to get the information so you can perform some task—and I explain how to get the information and what to look for so you aren't left guessing and have to research it yourself.

Now that you understand the goals of this book, let's look at why part of best practices says that security must be a business function.

Suppose you want to know more about your organization's human resources department, so tomorrow you and the rest of the IT staff go on a "tour" of that department. You find the file cabinets that keep all the employees' employment records,

and you start to look through them. In fact, you copy the records of some of the more "interesting" individuals—such as those of your manager, the CIO, and the CEO. Then you scan in these records and post them on your Facebook wall, or you tweet the more interesting bits to your followers.

Although this is an absurd story, it has more basis in reality than most organizations would like to admit. How many members of your IT organization have *ALLOBJ (all object) special authority or access to all production objects on your system? *ALLOBJ authority permits those employees to do electronically what they never would be permitted to do with physical file cabinets. If anyone other than the security administrator has *ALLOBJ special authority, you're permitting that person to violate a written or unwritten guideline that limits access to confidential or private data residing on your system.

Whether you're talking about locks on doors, restrictions on who can access documents in physical file cabinets, limitations on who can access files on your system, or controls over the information your company makes available on the Internet, your organization's policies—formal or informal, written or unwritten—govern your business. You must take those policies into consideration as you architect and implement your security scheme. If you make compliance with your policies a top concern, you'll go a long way toward being in compliance with many of the laws and regulations that govern your organization.

Evaluating Your Risks

It's quite fascinating to compare the amount of money that's invested in securing the physical hardware on which data resides with the amount of money most organizations spend on securing the logical access. In most cases, the amount spent on securing the logical access is miniscule compared with the investment in securing the machine room, when you consider the locked doors, raised floor, alarms, fire suppression equipment, and so on. Why the disparity? My hope is that this book helps raise the awareness that it's just as important to invest in the security of the logical access to the data as it is to the physical access.

As you evaluate the risk to your data, consider all the ways—whether accidental or intentional—in which an inappropriate disclosure, modification, or deletion of your information assets could occur. As you look at the risk, it might be helpful to identify it in terms of risk to the confidentiality, integrity, availability, and privacy of the data.

Confidentiality

Some information is obviously confidential because it consists of private information (such as payroll information) or because it could give a competitor an advantage (for example, early knowledge of an impending acquisition, quarterly financial results, proprietary product information, customer information, vendor lists). You must evaluate your data in terms of its confidentiality and value to the organization to determine how it should be secured. I'm certain you've heard stories about disgruntled employees who have stolen databases and sold the information on the black market. What's scary is how easy it is in most organizations to accomplish this deed. Given the way most systems are configured, some end users and most programmers could walk out the door of their organization's office with a copy of virtually any database file. Or they could email the information from the system or carry it home on a memory stick. How often are briefcases examined on the way out of your office? How many emails are scanned for inappropriate attachments being sent from your company? When it comes to restricting access to information assets, an organization's security implementation often fails.

Integrity

Information security also addresses the integrity of your applications and data. Applications and data must be authentic, accurate, and concurrent with your company's other applications and data. Problems such as order entry programs that lose order items, inventory control programs that introduce errors in replenishing stock, or item pricing records that someone has tampered with can easily bring a business to a crawl or standstill and can endanger profits and even the company's long-term success. You can't afford to risk the integrity of your applications and data because of a nonexistent or weak information security implementation.

For instance, if you let users share user profiles and passwords, you immediately sacrifice your system's ability to authenticate changes to information. In other words, the system can't accurately identify who is doing what on the system because one profile might represent several people. Although limited profile sharing may be acceptable for a specific application, as a rule system integrity requires you to prevent profile sharing.

What if users or management suddenly started doubting the accuracy of the data in your database? Perhaps someone mistakenly uploaded old data from a PC into a file. Or maybe a well-meaning programmer put into production a program that wasn't fully tested, which in turn introduced errors into the database. These two scenarios illustrate the importance of the integrity and accuracy of your programs and data. Your information

security plan must minimize the opportunities for users and IT staff to accidentally or intentionally introduce errors into your application repository or database.

Secure information assets are also vital to your company's integrity and reputation. Any security breach, when publicized, can harm a company's reputation. Say your business depends on the cash flow that its website produces, and you experience a highly publicized security breach in which consumers' credit card numbers are stolen. A well–thought-out and implemented security plan protects a company's integrity and reputation as well as its data. I've started to encourage my clients to take the attitude and assume they *will* be breached rather than hope that it doesn't occur. If you assume that a hack will occur, it's likely that you will take more seriously the security controls you put into place and take steps to ensure that you have set up enough layers of defense to protect your data and reduce your risk to an acceptable level.

Availability

You've probably heard the horror stories—or even experienced them yourself—in which production objects were accidentally deleted. Perhaps a developer thought he or she was deleting a test copy of a program, or a user accidentally hit the "upload" icon instead of the "download" icon and overrode the production sales file with data from a spreadsheet containing last month's sales data.

Regardless of the specific scenario, these types of disasters occur simply because users have too much authority to the data. If the user had sufficient object authority to download data but not to upload it, the possibility of overwriting production data wouldn't exist.

Although these disruptions are typically accidental, malicious attacks can also occur. Malicious or accidental, anytime data is not available to the organization, the organization is harmed. The degree to which it is harmed depends on what data is no longer available and on the length of the outage. A well-architected and -implemented security scheme can significantly reduce the potential of data being unavailable.

Privacy

Recent years have seen a dramatic rise in concerns about privacy, and numerous laws have been written to protect it. Consumers are becoming increasingly worried about how organizations use their personal data, whether it's collected over the Web, on an employment application, or in an electronic healthcare database. When data is gathered and inappropriately released (such as information collected from medical tests and credit

reports), individuals' lives are often adversely affected—either by sheer embarrassment or through identity theft or fraud.

Security alone doesn't guarantee privacy, but you cannot guarantee privacy *without* implementing good security policies and practices. Don't make the mistake of ignoring this area. Many countries, including the United States, Canada, and most of Europe, have legislation that mandates protection of personal information. Financial institutions in the United States must inform their clients about how private data is used and let them opt out of programs that may send that data outside the original institution. In the case of healthcare, the Health Insurance Portability and Accountability Act (HIPAA) requires physicians to tell their patients how private data is used and to obtain patients' permission before sharing that data with other physicians, healthcare organizations, or medical research teams.

Even if you aren't in a regulated industry, I strongly recommend that you evaluate *all* data your organization collects. If any of it is personal information, examine how it is used, ensure it is appropriately secured, and inform individuals (through your privacy statements) about how the data will be used so they can choose whether to give your organization their data.

Securing private data is a vital aspect of keeping private data private. However, it's important to realize that this is only one aspect of keeping private information private. Appropriately securing private data provides access control; that is, it determines who can see the data. However, security cannot enforce a policy of acceptable uses of the private data once that data has been collected or viewed. Nor can security enforce the policy of what data is actually collected. So just because you have the private data secured away from public access, don't think you've handled all aspects of dealing with private data. You don't want your organization to be the next Facebook when it comes to abusing the privacy of the information it gathers!

Another consideration is the aggregation of data. Some data, on its own, may not be considered private data, but when aggregated with other information, it's now private. For example, the State of California has determined that an email address is private data if it's kept in the same database as the answers to your password prompt questions. And the obvious issue of big data—not just the sheer volume, but the amount of data that can be collected on an individual or entity—must also be considered. In other words, you need to look at all uses of data across your organization and protect data appropriately.

Evaluating the Threats

What types of problems pose the greatest threat to your information security plan and implementation? A common thread you may have recognized in the scenarios discussed here is the role accidents can play in breaching confidentiality, accuracy, or availability. A sound security scheme provides significant protection toward reducing threats to your system. If you implement common-sense security measures, such as appropriately securing production data, securing source so that it cannot be updated outside of change management, reducing the number of all-powerful users, auditing the use of critical data and security-relevant actions, and handling data according to the requirements of its data type, you can eliminate many common sources of errors and omissions.

However, you cannot ignore the threat from disgruntled employees and hack attacks from literally all over the world. If you have never addressed security on your IBM i, now is the time. While it's doubtful you'll ever hear about an IBM i being hacked (because the operating systems and applications involved in a hack are rarely revealed), I can assure you that the IBM i *has* been hacked. Many people have a false sense of assurance that the system is secure. Rest assured that the system is secure-able—but the data on the system in not inherently secure, and you must implement the features provided by IBM to protect your system and data. One of the biggest threats to your data is complacency and ignoring the fact that steps need to be taken to secure the system. I see far too many managers and system administrators who continue to insist that they have nothing to worry about because their users are locked into a menu environment and/or their users couldn't possibly know how to access the system any other way than through a menu. These individuals couldn't be more wrong. Management's putting their heads in the sand and refusing to acknowledge the vulnerability of their data is, to me, the biggest threat to an organization's data.

Where do you start? First, develop a security policy; determine how risk-averse your organization is to having its data being lost, stolen, or unavailable; and then implement the appropriate security features to allay the risk.

Managing the Strategic Issues

Evaluating the risks and threats to your information assets is the key to getting management's attention. As you expose risks and threats, management begins to see the possible ramifications of inadequate or inappropriate security. Once you have management buy-in, it's important to follow through by implementing a security awareness program throughout your organization and ensuring that the requirements of

your organization's security policy are considered with all major changes that occur in the organization. In addition to managing upper management's knowledge and expectations of a security policy, you need to manage the access controls to your applications, data, and systems. And you need to establish and carry out security auditing procedures.

These tasks take time. But once completed, they provide the building blocks for the various security implementations you need to undertake for your enterprise's computer systems.

Control Access to Applications, Data, and Systems

Controlling access to your information resources involves physical security, managing user profiles and passwords, defining authorization roles, and implementing resource authorities and specific security programs to enforce and audit access to your system. This particular strategic issue constitutes most of the tasks usually associated with implementing security and consequently occupies the largest portion of this book.

In today's world, access control is a critical part of a security implementation. Perhaps in the past you relied on security measures, such as menu systems, to secure your own application users on the system. That method simply is not sufficient today. With numerous ways to access data that bypass traditional menus—such as File Transfer Protocol (FTP), Open Database Connectivity (ODBC), and Distributed Data Management (DDM), you must incorporate other approaches to ensure your data is secured appropriately.

One subset of access control relates specifically to security within the IT department. IT professionals are often oblivious to the need to secure the system from themselves. Some professionals perceive any form of security aimed at IT as, at best, making IT's job more difficult or, at worst, a personal attack. However, because security is a business function and the IT professional's tasks, like all other users' tasks, require security, IT security requires consideration and careful planning.

Some of the keys to a successful IT security implementation are apparent—committing to separate development, test, and production environments, for example. The production environment on your systems must be stable except for planned changes made using some type of change management system. IT professionals shouldn't have authority to production data and applications. However, there must be a contingency plan that provides access in the case of production emergencies.

IT vendors (e.g., consultants, third-party software providers) should fall under the same guidelines as in-house developers. They should have access only to development

and test environments. And, as in the case of in-house developers, all actions on production systems should be audited.

Red flags should be thrown and warning bells should go off in your head when third-party software providers require users to have *ALLOBJ special authority to run their software (unless, of course, it is security management software). *ALLOBJ should be the absolute exception and definitely not the rule. Make these vendors justify why users need *ALLOBJ special authority to use the software. There are some legitimate reasons for requiring *ALLOBJ authority, such as when an underlying operating system function requires it. However, no vendor should require *ALLOBJ authority simply to access the application's database.

Regardless of whether you're working with IT or end users, your security scheme should be formed according to the principle of "least-privilege access." That is, give users access only to those objects and capabilities that they need to perform their job function—never more.

Review Requirements and Maintain Compliance

In any security implementation, established security requirements and rules become less effective as time passes. Because your security requirements, as well as pieces of the system (e.g., the operating system, application programs, procedures) aren't static, you must periodically review and adapt your security plan to stay current with new threats, changing technology, and recently passed laws and regulations.

To maintain a security implementation, you must proactively monitor the compliance of your security implementation as well as review the security-related events that take place on your system each day. That is, you need to regularly check to make sure your implementation complies with your organization's security policy. Many organizations fail to review their policy and its implementation, instead simply trusting that the security implementation works and that "someone" will know when something isn't "right." Or, they choose to put their head in the sand and ignore the possibility that things may have changed.

Getting Started

The hardest part of implementing a sound security scheme is getting started. As you read the rest of this book, look for simple ways you can begin in your own organization. To do that, you must take these initial steps:

1. First, examine any potential risks to your company's information assets—that is, its data. Is there confidential or private information on the system that your company needs to protect? Can you guarantee the integrity of your organization's data? What would the cost be if this data were lost or stolen? To answer these questions, list the risks of your current implementation. Then, list the cost to the organization should the data be lost or stolen.
2. Next, obtain management support to begin documenting corporate-wide security policies. After defining the organization's policies, start to define the departmental procedures and establish data ownership. For information about writing a security policy, see Chapter 2.

Only after completing these tasks are you ready to begin implementing a new security scheme. It is in the enforcing that you'll use the technical tools described in this book.

The final step in getting started, from a management point of view, is to commit to maintaining your security implementation and plan. The only way to determine whether your implementation is working is to check the compliance of the current system settings against your security policy and continue to do so on an ongoing basis. When you discover gaps in the configuration, you can fix the implementation to bring it back into compliance with your policy.

The remainder of this book gives you the technical details and approaches for implementing security best practices for IBM i.

Technical Note

The operating system that is the subject of this book has undergone several name changes throughout its history. I use the current name, IBM i, but most of what you'll learn about in this book applies equally to recent versions of i5/OS and OS/400 (with the obvious exception of new functionality provided in V7R2 and V7R3). Similarly, I use the latest names for other IBM products and technology, such as Navigator for i (formerly iSeries Navigator), and my screen shots now reflect my use of Access Client Solutions (ACS) rather than Client Access client software, and other current technologies.

Don't Close the Book

Once you've written your security policy, evaluated your risks, implemented or reworked your security scheme, and tightened down your network, your job is done and you can toss out this book, right? Wrong. Security is a not a one-time event. I like to call it a "lifestyle." New technologies are introduced, new applications are installed, you upgrade the operating system, the organization acquires a new company or goes into another line of business. Because security is a business function, and the laws and regulations affecting how confidential and private data is used and secured aren't going away. Whenever your business changes or grows, you must evaluate those changes against the requirements of your security policy and then implement the appropriate security measures to ensure your organization's data remains secured appropriately and that your organization is still in compliance with its policies. In addition, you have to make sure, that amidst the chaos of change, you can effectively and efficiently administer the security of the system. So don't close this book! You'll want to keep it open for future reference.

Don't Get Overwhelmed

If you've found this chapter overwhelming because of the amount of work you see looming, I ask that you stick with the book. My plea is that you start somewhere with some task, be it large or small. Any change that you make reduces risk. So if this is new to you and you don't know where or how to start, don't be afraid to start with a few small tasks. It's far better than doing nothing at all.