

CHAPTER 2

DB2 Security— The Starting Point

FIRST WORDS—WHAT'S THE PLAN?

When thinking about organizational information security, your mind might jump to the technical details such as firewalls, access control lists, certificates, auditing, encryption, and all those well-known electronic trappings that present a mental vision of a secure architecture. In fact, if you review the security implementations for most organizations, you will indeed see all those things.

Did you ever wonder how those physical and logical layers of security ever started out? I did, and what I found out may surprise you. Despite all the electronic gadgetry, despite the fact that these environments were created by information technologists, despite this being the electronic age, despite the “paperless” society, the best security implementations ... the ones that still stand up to the test of time ... began as a written security plan on good, old-fashioned paper!

If you're seeking to emulate what other companies have shown to be successful, first you need to have a plan, and then you need to stick to it. That does not mean that you should create the security plan and never modify it, but it does mean that this plan should be solid enough to guide formulation of your organization's day-to-day database security policies.

In today's lightning-speed development and production environments, slowing down long enough to actually create a plan may appear to be an unaffordable luxury. Consider, however, that this plan does not need to be an impediment to progress, but rather an empowering document, facilitating the time and commitment of resources that must be dedicated to the security initiative.

If you happen to be a DBA, that written database security plan can be a lifesaver, both on initial database setup and as an ongoing reminder of the symbiotic relationship between the database and the security of the organization's information assets. It should give you guidance both before

and after a database has been launched. It will be an important guide as you formulate your DB2 database policies. It must be an active document, referred to for guidance on a regular basis and updated as change arises. For the corporation's sake, the database security plan should not suffer the fate of so many others and become yet another dusty binder stored on the top of someone's filing cabinet.

Perhaps, one of the most important benefits to be gained from creating a database security plan is that the very act of committing the plan to writing will assist in identifying potential security risks that might not be uncovered in a benign way otherwise. If security is not on the corporate conscious, the true threat is masked by all the tasks and energies required just to keep day-to-day operations or development going. Working on any security plan funnels the combined thoughts of the organization into one readable whole and presents in a clearer fashion the ways to address and mitigate those threats.

THE DB2 SECURITY PLAN

Because you're reading this book, it's obvious that you have an interest in protecting the data assets held by your organization; but unless you have a very small organization with a single very small database, you need a plan and a leader. Formalization of that plan will provide great assistance toward the goal of database security, and during the formulation of that plan, a leader (corporate sponsor) should emerge.

Many organizations already have some type of security plan in place that may or may not include specifics on database protection. If your organization has an enterprise-level security plan, the DB2 database security plan should be a significant and highly visible part of that document. If you do not have an enterprise level security plan in place, the DB2 database security plan should still be created, even if it must be undertaken as a standalone document. Given the criticality of protecting the data stored in those DB2 databases, ignoring the security responsibilities may mean unacceptable organizational risk.

The DB2 security plan document is a road map that will provide the foundation for the enforcement of the operational DB2 database security policies that will be implemented. It should provide a meeting of the minds with regard to the security of the organization databases and how DB2 should be used to fulfill those needs.

If you are a DB2 database administrator, you have a vested interest in getting a DB2 security plan in writing. This plan, once written and approved by management, can be your guideline for setting up your database security policies. It can be referred to when questions arise, such as access levels, provided to auditors to facilitate their reviews, and should be reviewed or revised when new applications are installed. A major bonus for you is that when finalized, it will keep you from having to answer the same questions about security over and over again, saving you time and allowing preservation of your sanity.

So, if necessary, take the lead on getting a committee involved in formalizing a written DB2 security plan. You may get resistance, but remember that the database you are trying to protect is potentially one of the greatest assets held in trust by your organization (and the people it serves), and, therefore, it should be treated and protected just as any other valuable corporate asset would.

Security Plan Meeting Participants

The first step toward achieving your database security plan is to identify the team members who should be involved in the creation and review of the document. In a typical organization, the positions listed in Table 2.1 might be considered key to this task.

Table 2.1 Database Security Plan Team Members

All Appropriate Members of Management
CIO
CTO
Vice presidents
Division managers
Technical team leads
Application subject matter experts (SMEs)
Network administrators
Systems administrators
Database administrators (DBAs)
Corporate security officers

One important factor in determining who to include is the realization that the matters discussed in these meetings could be used by internal or external sources in inappropriate ways. Because the focus of the meetings is to discuss and mitigate current and future threats, the core meeting group should consist of individuals who are trusted by the organization to maintain the confidentiality of issues discussed.

To succeed, the database security plan needs a corporate sponsor. This should be someone within the organization who has the appropriate level of interest, authority, and responsibility to approve, communicate, and enforce the resultant plan. If your corporation has a security officer, especially if the position that person holds has sufficient status within the organization, the security officer may be able to fulfill the sponsor role.

Obviously in large organizations, division personnel should be involved in the process. It is important to get their unique perspective on database security because they may face challenges that are not easily identified. Depending on your organizational structure, division technical personnel should be invited to the meeting if they have discrete environments or can provide technical expertise relevant to database or application security.

Communication and information from application SMEs will likely be necessary to determine the granularity of database security needed. These are the individuals who can indicate which data needs the most protection, which users should have access and the level of that access, and how to determine whether a breach has occurred. These individuals may be technical leads, application programmers, or just those who know the application well because of their role. For example, an accountant might be the individual who knows the most about the general ledger applications.

The remaining participants should be the hands-on technical individuals who typically have the roles of network administrator, system administrator, and DBA. Participation of individuals who fulfill these roles is absolutely critical to successfully designing a plan because each will bring a unique focus to the process.

Gather Information

Before any meetings are scheduled, there should be some gathering and summarization of information if it is not already readily available to the team. A minimum starting list of items includes the following:

- Current security documents
- Standards (formal or informal)
 - Any written security guidelines
 - Any informal security policies that have been enforced in the past
- Hardware in use or proposed for DB2 databases
 - Machine specifics
 - Physical location
- Connectivity mechanisms in use
- Current authentication methods
- Operating system information
 - OS type
 - OS level
- Maintenance procedures, such as patch management, currently in place
- Licensing agreements

- User and group information
- List of DB2 instances by hardware
 - The type of instance
 - Development
 - Test
 - Production
- The database manager configuration parameters in use per instance (DBM configuration)
- The product and level of the DB2 code base installed (DB2LEVEL command output)
- List of DB2 databases by instance
- Database configuration(s) (DB configuration)
- Backup procedures including types, frequency, and storage location
- Applications currently being run (as observed or proposed)
- Typical number of users
- Access control measures in place
 - Authorities
 - Privileges
- List of applications
 - Type
 - Web-based
 - Third-party
 - Batch
- Application “owners”
- Prior risk assessments
- Information on known data classification
- Special security considerations
 - Federated
 - Information Integrator
 - High Availability Cluster Multi-Processing (HACMP™)
- Results and recommendations of any security audits that have been performed

Meeting Goals and Desired Outcomes

After you get the appropriate parties and the initial information together, meeting goals should be established. It is difficult to create a database security plan in only one meeting unless your organization is very small, so it might be best to create overall goals and then plan enough meetings to allow time for discussion.

Segment the discussion with the idea that internal and external security may pose different threats and, therefore, require a different set of goals. Uniformity of standards can simplify security policies and should be considered to the extent that they can be implemented across the organization without incurring increased risk.

The result of these meetings should include a comprehensive, written policy addressing the components of the database security plan, including at a minimum, the following:

- A. Appropriate analysis of internal and external database security risks and the current approach toward their mitigation
- B. External security authorization mechanism
 1. Group and user naming standards
 2. Password standards and change guidelines
- C. Operating system standards (for DB2 files, file systems, logical volumes)
- D. A workable blueprint for setting up the DB2 database security policies

What security standards should be set for all databases?

1. A List of access control levels by database
 - a. Who needs access and at what level?
 - b. Granularity of access control needed
 - c. What security access is needed by the following?
 1. Application
 2. Group
 3. User
 4. Database
- E. Who will be responsible for internal user and/or group account setup?
 1. How will user accounts be tracked?
 2. How will terminations and revocations be handled?
 3. How will necessary access changes be conveyed?

- F. What approvals are needed?
 1. What forms are required?
 2. What sign-offs must be in place?
- G. Identification and classification of extremely sensitive information
 1. By database
 2. By application
 3. By table
 4. By column
 5. By row
- H. Identification of overall DB2 security management responsibility
 1. Who is the owner?
 2. Who can delegate?
 3. Who is the custodian?
- I. Uniformity of database policies and any acceptable deviations
- J. Auditing requirements
- K. Incident handling procedures
- L. The review cycle for the formulated database security plan
 1. Are there regulatory requirements for the review cycle?
 2. Should the entire plan be reviewed at once?
 3. Will there be a review after hardware changes?
 4. Will there be a review after software changes?

Meeting Facilitation Tools

When considering an analysis of internal and external database security risks, you can use a grid approach. Table 2.2 shows a basic example.

Table 2.2 Database Security Risk Grid Example

Internal	Threat	Plan
Shared passwords	High	New password policy.
Disgruntled employees	Medium	Review access levels before personnel actions are undertaken.

(continues)

Table 2.2 Database Security Risk Grid Example (*Continued*)

Internal	Threat	Plan
Users granted inappropriate access to data	Medium	Check and review current database grants; create an access control policy.
External	Threat	Plan
Introduction of vulnerabilities due to lack of maintenance	High	Schedule maintenance window for patches.
Hacker attack	High	Keep current with patches; encrypt sensitive data; change passwords on a regular basis; enforce password standards; undertake vulnerability assessment.
Web users with incorrect access	High	Check and review current database grants; create an access control policy.

It is likely that this grid (or any other facilitation mechanism used to capture this detail) can grow quite large. It should be viewed as a brainstorming tool to assist in determining the scope of risk. As in the example, it is likely that the items under the Plan column may contain duplications that might occur when one risk can be mitigated by the same action as another risk. An example of this is a risk of external resources and internal resources holding inappropriate access to data. Whereas each presents a different threat to the database and potentially a different level of risk, one action that should be included in the plan for proposed mitigation of both is to review current database access levels and create an enforceable access control policy.

The formation of this grid may assist in identifying the highest-priority items that should be addressed first (even before the plan is completed) and might lead to discovery of threats not currently on the corporate radar. As a first step before tackling the robust work of actually formulating the part of the plan that will serve as a blueprint for the DB2 database security policy, the grid will facilitate an assessment of where the corporation stands now with regard to database security and potentially assist in identification of any serious lapses.

After the assessment of internal and external threats has been completed, the results should be summarized and organized to be used as input for the next steps.

Determining the Authentication Method and User/Password Security

Authentication for DB2 databases is handled by a security facility outside of DB2, such as the operating system, Kerberos, or other plug-in. Although it is not necessary at this point in the process to be specific as to the parameter settings (authentication is discussed in detail in Chapter 5, “Authorization—Authority and Privileges”), the overall authentication requirements should be documented. The discussion should include a determination as to where the authentication

should take place (that is, client, server, DB2 connect server, host) and whether encryption (Chapter 7, “Encryption [Cryptography] in DB2”) is required.

Standards should be developed for naming conventions for groups and users. Part of this strategy should be that known default or easily identifiable group names and usernames are not allowed. Some that are commonly used in many DB2 shops (and should therefore be avoided) include the following

- db2admin
- db2as
- db2inst1
- db2fenc1

Another important discussion regarding groups revolves around the DB2 group known as **PUBLIC**. DB2 comes with this group by default. This group can (and should) be locked down unless there is some documented reason for this group to maintain certain low-level privileges. Prior to DB2 9, this group always received a number of privileges from the moment the database was created. With DB2 9, an alternative for dealing with the **PUBLIC** group privileges is made available. When creating a new database, adding the keyword **RESTRICTIVE** changes the default behavior, and no privileges are automatically granted to the **PUBLIC** group. If this keyword is not used, the following permissions are available to the **PUBLIC** group after the database has been created:

- **CREATETAB**
- **BINDADD**
- **CONNECT**
- **IMPLSCHEMA**
- **EXECUTE** with **GRANT** on all procedures in schema **SQLJ**
- **EXECUTE** with **GRANT** on all functions and procedures in schema **SYSPROC**
- **BIND** on all packages created in the **NULLID** schema
- **EXECUTE** on all packages created in the **NULLID** schema
- **CREATEIN** on schema **SQLJ**
- **CREATEIN** on schema **NULLID**
- **USE** on table space **USERSPACE1**
- **SELECT** access to the **SYSIBM** catalog tables
- **SELECT** access to the **SYSCAT** catalog views
- **SELECT** access to the **SYSSTAT** catalog views
- **UPDATE** access to the **SYSSTAT** catalog views

As you can see, the privileges for the **PUBLIC** group on a newly created database are significant. If discussions yield no valid reason for **PUBLIC** privileges, the **RESTRICTIVE** clause should be used for newly created databases.

Excellent password security is one of the elements of a strong security plan. In addition to identifying the responsibility for password security enforcement and the mechanisms for change, the following topics should be considered:

- Changes
 - Will users change their own passwords?
 - If not, how will they be notified of the changes?
- Length of time between required resets/changes
 - If not reset/changed, how long until lockout of the account?
 - How many cycles must be completed before passwords can be reused?
- Resets
 - Who will hold responsibility for password resets?
 - Will a secondary authentication be used to allow the user to reset it?
 - Secondary authentication question answered correctly
 - Biometric authentication
 - Electronic device such as a key card
- Lockouts
 - How many password attempts before lockout?
 - What forms and approvals are to be in place?
 - Who will have the authority to retrieve a lost password or credential?

In considering passwords, a discussion of composition standards for those passwords is necessary. The human factor in password issues is well recognized. If your users are allowed to create their own passwords, without any applicable standards, the strength of those passwords will be suspect. If complex passwords that are not easy to remember are instead assigned to users, invariably they will be written down someplace, and that overrides the strength of the complex password.

One approach to this is to create a security password template. This provides the mechanism to ensure that the password meets certain standards, such as three capital letters, two numbers, one symbol, and two lowercase letters. However, this can be problematic. Consider that internal employees will know the template. This information could provide an unintended assist if an internal or former employee wanted to gain access through password hacking.

It is critical that forbidden passwords include usernames, employee IDs, dictionary words (in any language), and true words with numeric replacements of ones or zeros. All these are easily hacked by a brute-force approach.

It's easy to say that passwords should never be shared, but harder to enforce that standard unless there is some strength behind the security plan, policies, and procedures that can bring consequences to those who violate this essential security foundation. Passwords should also be expired, but this brings up the question "When?" Too-frequent password expiration is problematic because users are tempted to write them down somewhere. A longer time between password changes means a longer exposure period. Changing passwords on a regular interval can be beneficial, but if this actual interval is widely known, this, too, can be a risk. Would you really want a hacker to know that passwords expire on the first Saturday of every other month? Encryption of all passwords is a strong recommendation. DB2 provides easily implemented encryption security features to protect passwords (and more), as discussed in Chapter 7.

As with all security features, knowledge of current industry standards and practices regarding password topics will provide the best guidance. As security evolves, so do the attempts to thwart that security, so keeping current through a proactive approach is wise.

Discussing the Blueprint

Now that you have summarized the results of the internal and external risk assessment for database security and addressed authentication, it is time to begin work on the part of the plan that will eventually be used as a foundation for creating the actual DB2 database security policies. At this point, the team needs to have a good understanding of the internal and external threats that should be addressed to protect the database.

During this phase of the meeting process, the team should begin to discuss the security standards for all corporate DB2 databases. Depending on the structure, complexity, and size of the organization, this can be intricate with multiple considerations per division, per database, per machine, and so on. The goal of this part of the plan is to integrate information discovered in previous steps to facilitate creation of the DB2 database security policies.

At this phase of the process, the team should begin to discuss a workable set of security standards and how they should be applied.

Questions to be answered and topics to be codified in the plan include the following:

- The ability to uniformly apply database security standards
 - Are there needs for differing standards based upon ...?
 - Divisions
 - OS types and levels
 - File system storage versus raw devices
 - Firewall

VPN

Federated

Replication

LDAP

Are there special considerations for specific third-party applications?

If so, how will these differences be identified and handled?

- Access control plan

A statement identifying responsibility and ownership

Account/group setup

Account tracking

Terminations

Changes

Matrixes of access levels needed (see Table 2.3)

For authorities

For privileges

Special

Identification of necessary maintenance steps

Approvals

Forms

Sign-offs

- Identification of extremely sensitive information for special consideration

As mentioned previously, matrixes can aid in identifying access requirements. You can then use these matrixes as input for the DB2 database security policies. The examples in Tables 2.3 and 2.4 consider specific access levels and decode, by group, the level(s) that should be applied. Although the examples represent true discussion points, the values assigned here are for a fictional company, and no special meaning should be ascribed to them.

Table 2.3 Database Authorities Matrix

Instance Level	Corporate Tech Arch Group	Corporate DBAs	Division 1 Tech Group	Division 1 DBA Team Lead	Conversion Team
SYSADM	Y	N	N	N	N
SYSCTRL	N	Y	N	Y	N
SYSMAINT	N	Y	Y	Y	N
SYSMON	N	N	N	Y	N

Database Level	Corporate Tech Arch Group	Corporate DBAs	Division 1 Tech Group	Division 1 DBA Team Lead	Conversion Team
DBADM	N	Y	Y	Y	N
LOAD (with insert privilege)	N	N	N	N	Y

Table 2.4 Database Privileges Matrix

	Public	All Groups	Software Development	Conversion Group	ETL Group
Connect to database	N	Y	Y	Y	Y
Create new packages	N	N	Y	Y	Y
Create tables	N	N	N	Y	N
Unfenced stored procedures or UDFs	N	N	N	N	Y
Implicitly define schemas	N	N	N	N	N
Connect to database that is in quiesce state	N	N	N	N	Y
Allow user to create a procedure for use by other applications or users	N	N	Y	Y	Y

Definitions and detailed explanations of authorities and privileges are covered in Chapter 5.

You can build similar matrixes to assist in identification of the additional security privileges to be addressed in the DB2 database security policies. These could include the following:

- Schema
 - Create objects within the schema
 - Alter objects within the schema
 - Drop objects within the schema
- Tablespace
 - Create tables in a specific tablespace
- Tables and views
 - Control of a table or view
 - Add columns

- Add or change comments
- Add a primary key
- Add a unique constraint
- Create or drop a table check constraint
- Select, insert, update, and/or delete rows
- Create indexes
- Export
- Create and drop foreign keys
- Packages
 - Rebind
 - Execute
 - Allow package privileges for others
- Drop and control on indexes
- Execute routines
- Use and alter on sequences
- Passthru (in a Federated database environment)

Next Steps

Now that the plan has been visualized, it is time to put it to paper. In thinking about what has been covered, it should be obvious that some of the information provided in this living document could be sensitive in nature. It is detailing how your corporation plans to mitigate security risks for the database and, therefore, could provide information to hackers or an internal employee and become an unintended aid for the very risks the plan is meant to address.

Think about the “security” of the database security plan document. It should be protected while it is being written. Leaving parts of it lying around while it is being typed is not appropriate. The persons doing the typing should be trusted employees, too. At a minimum, the electronic copies of the plan should be password protected.

Because of the sensitivity of the information, it is best to disseminate the plan on an “as needed” basis. One possible scenario is to create a security library with all security documentation provided through a signed checkout process. Other steps such as limiting the use of the document to one room that does not have a copier and stamping each page with a highly specific watermark to verify authenticity could provide some measure of further security.

DB2 DATABASE SECURITY—CREATE THE POLICY

DBAs are notoriously overworked. They are an integral part of the day-to-day database management work and serve as the technological wheels of the corporate vehicle. Given their usual desire to stay “hands-on” and the significant tasks that they face, DBAs seldom have the time or inclination for writing documentation. When security is not a priority, database security policies, if they are documented at all, are often vague and will likely suffer from poor implementation. Given the considerable security risks imposed by ad-hoc policies and spotty enforcement, committing the policies to writing and implementing them consistently and successfully is critical.

Although a trial-and-error learning approach might work in some database areas, database security is not one of them. It is critical that the DBA who is tasked with creating and implementing the policies understands, and can intelligently implement, all aspects of the DB2 security policies. Auditing is another area that requires a robust comprehension of DB2. For these reasons, the database security policies should not be created or implemented until the DBA has a true comprehension of the available DB2 security options.

Using the Plan to Formulate the Policy

If the DB2 database security plan is complete, the creation of the DB2 database security policies will be much easier. Yes, it is true that a database security policy can be put in place even though a database security plan was never created. However, creating only the policy without first laying the foundation of the plan leaves the database policy vulnerable. For example, there might not be a corporate sponsor to favor the necessary work effort, organizational “buy-in” would be missing, and database security efforts would not benefit from the strength of different perspectives.

That said, if it just is not possible to get a team together and officially write a database security plan, at least writing the database security policy is the next best choice. Plan or no plan, the DB2 database security policies should be written down, not just implemented.

Review, Approve, Implement, Maintain

Before sitting down to translate the information from the plan into workable database security policies, a structure should be in place to determine what reviews, approvals, auditing, and policy maintenance are needed. The goal here is to strengthen the process, not impede it.

If the corporation has a technology security officer or group, that group should be part of the review, approval, and maintenance process. If no individual or group holds this authority, the CIO or CTO and/or DB2 team lead should be involved. Rather than have numerous levels of authority

involved, the objective is to find the smallest common denominator of personnel with the appropriate level of authority and the ability to do the following:

- Review the policies
 - Do they match the objectives of the plan?
 - Are the proposed policies able to be implemented as they are described?
 - Are the appropriate parties tasked with implementing the policies?
 - Are safeguards built in?
 - Is the policy clearly written?
 - Has change management been addressed?
- Approve
 - Who has the authority to approve the policies?
 - Are multiple levels of approval desirable?
- Implement
 - Identification of personnel to implement
 - Verification of successful implementation
 - Appropriate change management
- Audit
 - Validation
 - Quality assurance
- Maintain
 - What is the schedule for cyclical review of the policies?
 - Who will maintain the physical security of the policies?
 - Who will be allowed access to the policies?
 - How will the policy itself be distributed and secured?
 - How will changes be managed?

General Guidelines—Building the DB2 Database Security Policies

When beginning to create a new DB2 database security policy, a good suggestion is to have a master document that supports all the standards and single or various subdocuments to address the exceptions or differences. This approach may ease regulatory compliance efforts because uniformity across environments will aid auditors as they review for compliance.

One direction would be to create a master DB2 database security policy that covers all corporate instances and databases by stating the general, shared policy rules. Then, any exceptions or differences could be detailed separately and incorporated into the policy documents. The master

document might contain items such as the standards and naming conventions for instances and databases or how TCP/IP port numbers for instances are assigned. These are just examples to provide “thought points” for the task of creating the policies. As long as the written policies provide sufficient scope and clarity, the actual form that the final documentation takes is not significant.

One major point to consider is how to keep the policies themselves secure. The security plan and policies and their working documents, if made available inappropriately, present a security threat to the organization. If the policies are stored on a network that does not provide sufficient security, for example, they might be compromised and used as a blueprint to devise ways to circumvent all the protections so diligently implemented. Likewise, copies of the security policies or their drafts, left lying on desktops, can be acquired improperly. Keeping the plan and policies secure is just as important as keeping the data itself from falling into the wrong hands.

What to Include?

The determination of what to include and exclude in the database security policies varies greatly depending on the organizational need. Common to most organizations are items such as naming standards, database-to-storage mappings, application-to-database mappings, and access controls. Beyond those topics, larger organizations typically need to include auditing and encryption, especially if they are under regulatory review.

These topics are discussed in general terms here to give some insight on an approach to creating the policies. These topics are indented only to provide a starting point to initiate the process. The successful database security policy at your organization will be unique and a “custom fit” that cannot be easily facilitated by a generic blueprint.

Naming Standards

The most important considerations for creating naming standards are that

1. They exist.
2. They are not overly complex.
3. They are well documented.
4. They are not so transparent as to aid a hacker.
5. They are enforceable and enforced.

Organizations without naming standards cause undue stress for DBAs whether in relation to security or not. It is so much easier, for example, to troubleshoot any security issues with stored procedures if the DBA knows that all stored procedures begin with the prefix `SX_` and that they all are stored on a specific file system. If objects suddenly appear to be stored procedures, but do not begin with `SX_` and are not on the appropriate file system, the irregularity is more easily discovered if standards are in place and if enforcement has been strict.

Mappings

While database, application, and storage mappings exist in most organizations as an aid to administration, the implicit security benefit is not always realized. Mappings can prove invaluable to facilitate identification of irregularities (whether accidental or intentional). If a recovery is required for any reason, you can use mappings to confirm that the environment is restored to the original configuration. Mappings for applications, databases, and storage should be included in the database security policies.

Access Controls

DB2 offers a rich complement of features that can provide a high level of granularity for enabling access controls. Because a thorough understanding of DB2 access control mechanisms is critical to a secure implementation, these topics are covered in depth in Chapter 5, and Chapter 6, “Label Based Access Control.”

Once determined, access control mechanisms should be thoroughly documented in the database security policies. The goal should be a standardization of implementation that can be followed by anyone tasked with the work. The policy should spell out not only the initial implementation, but how to handle subsequent implementations.

Auditing

Another item for inclusion in the database security policies is auditing. (See Chapter 9, “Database Auditing and Intrusion Detection,” for a detailed discussion.) As you read in Chapter 1, “The Regulatory Environment,” auditing is a requirement for compliance mentioned by HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley Acts. Many governmental agencies require an almost 100 percent auditing implementation. If auditing is required, whether natively in DB2 or by some other mechanism, this, too, should be detailed by the database security policies.

The broad topics regarding auditing that the policy should (at a minimum) include are as follows:

- What is audited?
- How often will audit records be reviewed?
- What personnel will be tasked with audit review?
 - How will they be vetted or authorized?
 - What technical skills will they need for the tasks?
 - Who will they report to?
- What storage media will be used and how will it be secured?
- How long do audit records need to be kept?
- What is the issue discovery reporting process?

Auditing might not be required for every database environment in the enterprise, but to the extent that it is, it should be well documented in the database security policies.

Encryption

If your organization is planning to use encryption, the database security policies should address how to determine which data is to be encrypted. It is more important to set *standards* for encryption rather than just list specifically what is initially encrypted. If the policy states, for example, that Table A, Column B must be encrypted, that provides instruction only for one situation. The policy should go further, setting standards that apply across all data, such as the following:

- All names
- All Social Security numbers
- All dates of birth
- All personnel actions
- User IDs and passwords
- Credit card numbers
- Etc.

Spelling out this information in the policies is necessary because few applications stay static. As new code is introduced and new database objects are created, the database policies can aid in providing a consistency point for encryption. If the requirement is that all SSNs be encrypted, for example, and the policy only states, “Encrypt all Social Security numbers in the Employee table,” what happens when another table is added that also holds Social Security numbers? With standards such as “All SSNs are encrypted,” there is more assurance that the policy will be effective.

CHANGE CONTROL—THINGS ARE GONNA CHANGE

Throughout this chapter, we have been dealing with the “present” as if the “future” were never going to impact the process. Now it is time to realize that the future is not going to be ignored forever.

It is highly likely that after the plan has been completed (or maybe before), after the policies have been “inked,” and after that secure database is in place, there will be changes. With any security implementation, there are always ways to improve, which translates into “change.” Then, there are the business changes that occur as a matter of routine for most enterprises. They also spell “change.” We cannot forget, too, that technology will advance, hackers will hack, businesses will acquire businesses, best practices will evolve, and employees will move on. To manage the change that is virtually guaranteed in any thriving enterprise, change control is essential. This is not just change control for the database (although that is essential), but also change control for the security architecture and its relevant documentation. At each step along the way, consider how change is going to be managed.

LAST WORDS



If you do not have executive sponsorship for your secure implementation, *stop here* and get it now. Without executive sponsorship, the odds of success are slim.

Security plans and database security policies are essential to creating and maintaining a robust security implementation. They must be effectively written, shared with appropriate personnel, updated when appropriate, and protected just as if they were classified data. They serve as documentation for auditors, management, and appropriate staff and will provide foundational guidance for DBAs and IT departments.

Of course, every organization is different, and the security plan and database security policy must be tailored for the specific organizational need instead of striving to meet some arbitrary set of requirements. That is why the involvement of the appropriate personnel at the start of the creation process is crucial. These stakeholders should play an active role in the formulation of the plan, and from the plan, it should be easier for the DBAs to formulate the DB2 database security policies.

Taking shortcuts by eliminating documentation introduces significant risk. Even if database security is effectively implemented, when documentation is bypassed, it is increasingly likely that normal changes, which inevitably take place as the application changes, will cause security items to be overlooked. With a security plan and DB2 database security policies, this unintentional oversight is less likely.