Foundation for HP Data Security

INTRODUCTION

Data security is an issue for any organization relying on HP3000 computers. Assets such as operating systems, applications and data files exist irrespective of an entity's size or purpose. Although the degree of any given file's sensitivity and recoverability varies, an expense is attached to any data that must be recreated.

These statements are as applicable to relatively small HP3000 users as they are in State Farm's case. However, the degree of applicability may be greater for State Farm, as it develops a network of hundreds of HP3000s to support and perform the sensitive task of insurance claims processing. The fact that application and network development were underway several years prior to any coordinated data security effort further complicates matters.

Consequently, substantial effort has been expended over the past three years of our HP data security program to "catch up and keep up". While I would not claim that State Farm has the ultimate HP security strategy for every other organization, our approach's effectiveness is due to a foundation of components that I feel should be considered by all other programs. Hopefully, the HP data security directions and experiences that follow will lend benefit to your company's computer security program.

BASIC GOAL IDENTIFICATION AND STRATEGY

Any project or task addressed by State Farm's HP data security program is undertaken to further at least one of the following two goals:

1. A user's system access and activity should be uniquely identified.

2. A user's computer, application and file access should be limited to only those resources necessary for satisfactory job performance.

Transforming these statements from philosophy to HP security practice in a large HP operation can be a time consuming, frustrating, misunderstood and political process. While developing an HP3000 data security program can sometimes be an unnerving experience, I have found that its negative possibilities can be greatly diminished through coordination of the following components:

1. Security administrator education

2. Exposure identification

3. Management backing

4. User awareness

5. System access control

6. File access control

The presented order of these six points is deliberate. As much as is practical, for example, I feel that security administrator education should precede all other aspects of the program. As a further illustration, I believe that implementation of any computer-based access control must follow management approval and user awareness. With the advance understanding that none of these six security building blocks can stand on its own, the following sections explore each of them in greater depth.

SECURITY ADMINISTRATOR EDUCATION

State Farm was almost exclusively an IBM shop for many years prior to the entrance of HP3000s onto its scene. Consequently, like many analysts "on the HP side" today, my background was that of an IBM application programmer. I had much to learn about MPE and State Farm's usage of HP3000 systems before I would be competent to lead any effort to improve my company's HP data security program.

MPE Education

My formal HP educational background consists of the "Programmer's Introduction" and "System Manager" classes. The former served as a satisfactory primer on topics such as system access commands, UDCs and file access security matrices. Roughly half of System Manager focuses directly or indirectly on security issues such as file access control and the power of PM and SM capabilities.

Informally, I have tried to tone my HP security awareness through such references as the Systems Operation and Resource Management Reference Manual. This resource notes the functions of the various MPE capabilities and details the purpose and usage of relevant MPE commands (like NEWACCT).

HP's Communicator manuals, published with new releases of the operating system, can also be an excellent source of data security-related information. One of the most helpful MPE enhancements in our data security effort was disclosed in the UB-Delta-1 Communicator. It stated that U-MIT would allow an SM-capability userid to perform all userid and group maintenance, discontinuing the security administrator's prior need to access the systems via hundreds of AM-capability userids assigned to the various accounts.

Data security-related articles in periodicals such as INTERACT and The HP Chronicle have also presented a wide range of facts and commentary. I'd like to close by noting one of the newest MPE educational tools: the MPE/XL Account Structure and Security Reference Manual. While identifiable with MPE/XL, the data security practitioner should find nearly all of its content applicable to MPE and nicely encapsulated in this functionally specific resource.

Organizational Education

Effective HP data security administration required that my operating system education be coupled with a familiarization of State Farm's HP3000 usage. This process began with orientations conducted by other HP-related areas, committee work and informal conversations. Through these experiences, I began to generally understand our HP program's strengths and weaknesses, and what area's were responsible for the various support functions (teleprocessing, system performance, application development, etc.).

The organizational understanding attained through these experiences has proven to be a key factor in reducing State Farm's HP system exposures. For example, several areas have agreed to relinquish their PM and SM capability assignments, alternatively allowing analysts in the system management area to perform sensitive tasks (e.g., file updates in the SYS account) for them.

What follows is a sampling of data security-related topics relative to State Farm's HP3000 usage. While the associated responses are unique to my environment, I invite you to consider what your answers might be. The point of this exercise is to develop a "big picture" of the challenges that your data security program faces:

What primary business purpose(s) does my company's HP3000s serve?

The automated processing of insurance claims.

What is my company's policy on PM/SM capability availability?

Availability should be as limited as practical. This policy also applies to PM-prepped program development. The negative potentiality of PM and SM on system security is too severe to tolerate passive assignment of these capabilities.

Have other areas been designated to assist in the HP security administrative effort?

1. Each of State Farm's twenty-five regions has at least one data security administrator. However, his/her responsibilities also span to the IBM systems. In addition, these administrators currently possess minimal HP security background and few software tools to effectively maintain a security program.

2. Users are responsible for the security of their userid(s). However, many users currently lack the HP security education and password assignments necessary to protect their userids to even a minimal degree.

Where are my company's HP3000s located?

State Farm's HP systems are located in restricted areas of its corporate headquarters, regional offices and larger claims service centers.

What are my company's most sensitive HP3000 files?

1. Claims-related databases

2. Operating systems

3. Teleprocessing systems

4. Electronic mail systems

What is my company's HP userid policy?

1. Userids should be unique in the session name- or user-level qualifier and be identifiable within a given individual or process.

2. Userids should be password protected.

3. A user is responsible for all system activity via his/her userid.

4. For security reasons (ironically), most users lack the AM and/or SM capability assignment necessary to maintain their own MPE password(s).

Data Security Education: A Closing Thought

A final point about HP data security education: the process never ends. I found that it is all too easy to formulate security policy based on an educational plateau, failing to invest time to additional research that may result in reevaluation of current practices. For example, PS (Programmatic Sessions) capability's availability was restricted until further investigation revealed that it did not grant its user carte blanche access to the systems through the userids of others. I feel that the data security function owes a duty to its organization to reexamine its policies in light of improved understanding and changing conditions.

MANAGEMENT BACKING

Just as many of State Farm's HP analysts have IBM "roots", so too does our data processing management structure. In many instances, DP management is responsible for pursuits in both the HP and IBM environments. Even in those areas totally committed to HP3000-related development, managers are often too busy with their areas' respective responsibilities to devote much if any time to data security issues.

Given this scenario, it became clear at an early stage that the success of State Farm's HP data security program was very dependent upon management's appreciation of the issues. I have delivered the message in various forms. For example, an article detailing the data security ramifications of PM and SM capabilities was addressed to all first-line DP managers with HP-related responsibilities. I have discussed the power and public nature of the MANAGER.SYS userid with the manager responsible for operating system integrity. (He now maintains his own list of authorized MANAGER.SYS users.) In varying degrees, several managers became involved as their areas relinquished their PM and/or SM capability assignments. A memo

briefed a data processing vice president on the exposure to our regional office HP3000 exposure caused by Corporate analyst access to our X.25 network-connected Corporate gateway computer. Admittedly in varying degrees, presenting management with issues such as these as resulted in endorsement of our HP data security program.

Last mentioned but far from least important is the backing of my data security manager. Of all of State Farm's DP management, he has unquestionably been the most important individual for me to brief on HP security developments. This practice has not only helped him promote HP data security at his organizational level, but it has also enabled him to more effectively critique my ideas.

As I have stated, State Farm's HP data security program has had a lot of "catching up" to do. Sensitive capability assignments and obsolete userids have been removed, file access has become more restricted, etc. Management education and backing has greatly facilitated these sometimes delicate processes.

USER AWARENESS

I have seen examples of impressive data security awareness pamphlets, videos, etc. While I soon hope to pursue these more structured user awareness techniques (e.g., HP data security seminars for trainees and for on-board personnel), our area's priorities and staffing have dictated more informal approaches to date. Examples of these follow.

Committee Work

Committees can offer an excellent opportunity to express security-related opinions and suggestions, often at the assigned task's ground level. Committee charges in my environment have included dial-up procedures for non-State Farm users, userid implementation on new systems and HPDESK password procedures for regional office users. Analysts from a spectrum of other functions are exposed to security concepts in this manner. Committees are also an effective vehicle when the primary topic is HP3000 data security (e.g., security software evaluation, procurement/development and implementation). This latter case has rendered the added benefit of allowing others to participate in and understand State Farm's HP security direction.

Security Articles

This approach can make HP security a much less bitter pill to swallow. In a totally non-confrontational manner, users can learn more about their HP3000 environment and its security function. I have written articles on the security implications of PM/SM/OP/AM capabilities, group passwords and accounts without userids. A future topic is the comparison of our third-party system access security package with MPE. I would also like to explore the benefits and drawbacks of released files in an educational article.

Implementation Announcements

Third-party system access password implementations are in progress for State Farm's Corporate users. Rather than simply activating these passwords, I mail explanatory memos to the affected analysts a couple of weeks in advance. The notice details how the password will be implemented (e.g., on user-level qualifiers, (the "MANAGER" in MANAGER.SYS) or on specific session names of a user-level qualifier), illustrates what the new system access process will look like and explains how to change the password value. This vehicle has allowed users to become more aware of their HP system security responsibility without becoming confused and irritated with new procedures.

Informal Conversations

One-on-one telephone conversations or break area discussions can facilitate user awareness. This vehicle is more personal than memos, and it may be more appropriate than the committee setting for ad hoc HP security issues. In addition, sensitive issues can be dealt with in confidence. As an example, I have found this approach very useful when persuading users to relinquish their assignment of sensitive system capabilities. Rather than risking user embarrassment and/or resentment via the committee or memo approach, many sensitive capability assignment have quietly been eliminated.

Closing Comments

As much as practical, you want a supportive user base for your HP3000 data security program. Even with management's backing, your efforts will only result in a lukewarm level of effectiveness if your users are indifferent or opposed to them. Finally, it is humanly and programmatically impossible for me to notice every HP security shortcoming in a network as extensive and dynamic as State Farm's. I (and probably you) need to draw on users' expertise to flag exposures missed by standard security procedures.

SYSTEM ACCESS CONTROL

HP3000 system access control at State Farm rests on a developing foundation of security administrator experience, management backing and user awareness. These three factors coalesced in meetings of representatives from the various HP areas. In the early stages of discussion ,it became clear that State Farm's usage of HP3000s necessitated a software solution beyond the access security capabilities of MPE.

I'll begin by examining MPE's system access security shortcomings relative to State Farm's needs. My company supports a system access security policy of centralized creation, modification and deletion of userids, but decentralized password maintenance responsibility. Unfortunately, MPE requires that the userid and password functions either both be centralized or decentralized. In other words, AM and SM capability assignments may be severely restricted, with the controlling area responsible for userids and passwords. Alternatively, these capabilities may be widely available, with the various areas able to attend to their own userids and passwords. (In the latter case, however, HP3000 access security is based on the honor system at best.) Additionally, State Farm promotes a standard of user identifiability for all HP3000 access. For userids like MANAGER.SYS, system access uniqueness must be derived from the session name-level qualifier (the "KELLY" in KELLY,MANAGER.SYS). Unfortunately, MPE cannot require usage of the session name qualifier. Finally, in the absence of HP's Security Monitor product, MPE passwords are unencrypted. AM and SM capabilities can be abused to disclose the MPE system access passwords of others. Once again, this MPE feature's effectiveness is reliant on the very restricted availability of AM and SM capabilities.

To address these system access security drawbacks, State Farm recommended a third-party vendor product to enhance MPE. It disallows system access to unauthorized userids. While centralizing userid administration, the package decentralizes password maintenance. Users may be allowed to change their own vendor and MPE passwords, regardless of AM/SM capability assignment. The software also may enforce the supply of specific session name qualifiers at system access. Vendor passwords are encrypted and may be assigned to both the "user.account" and "session name,user.account" formats. Finally, security administration is not conducted through the MANAGER.SYS userid. Therefore, the userid upon which a system's access security is based need not be shared with areas responsible for other system management functions.

Simply implementing unique userids and encrypted passwords upon an HP3000 network like State Farm's is a sizeable task (well over 10,000 userid profiles are administered at Corporate Headquarters alone). However, the chosen access security product also provides for future "fine tuning" with features such as time-of-day restrictions, port restrictions and userid deactivation. These options, plus expanded usage of the product's reporting capability, will continue to strengthen the system access control component of State Farm's HP3000 data security foundation.

FILE ACCESS CONTROL

At State Farm, the HP data security administrator's job doesn't stop at the system gate. Whether uniquely identified or not, no HP3000 user is authorized to access all MPE files in all modes. System managers are not supposed to be reading the electronic mail of others. Programmers have no authority to recompile vendor code. No State Farm user is to be using TELESUP files from the TELESUP account. (We have established a separate account loaded with authorized TELESUP files for analyst use.)

Security administrator education in the area of MPE file access control is very important at this point. File access is determined by a matrix of account-, group- and file-level rules. Examining a single array of the matrix is most often misleading. For example, a particular file's file- and group-level access arrays may specify that any system user can take any action with that file, but the account-level array may limit some or all modes of the file's access to users logged into the file's account.

Security administrator education in the area of file access control must also extend to MPE's limitations. Matrix research via MPE is limited to the LISTSEC command in MPE's LISTDIR5.PUB.SYS (or "LISTF filename,4" in MPE/XL). On HP3000s like State Farm's, possessing millions of MPE files, an effective matrix evaluation via operating system tools would be impossible. Even a regular file examination of key accounts like SUPPORT, SYS and TELESUP would require a prohibitive time investment. Yet, with every system user able to identify every file via LISTF @.@.@, such regular, thorough access evaluations should be conducted.

Once again, State Farm has chosen a third-party vendor product to enhance its HP3000 file access security program. The software is used, for example, to flag released files. Another application may be identification of those PM-prepped program files with system-wide WRITE access. Scheduling these reports to be generated on a regular basis further strengthens this component of State Farm's HP data security program.

But what about identification of "mysterious" file creation, modification or deletion? We have a program that uses the system log to remedy these situations. It summarizes userid file activity or file usage regardless of userid for a given day or week. Hopefully, the aforementioned efforts to appropriately limit system and file access will diminish the need to invoke this utility.

CONCLUSION

From a very humble beginning, State Farm's HP3000 data security program has, by necessity, progressed rapidly to uniquely identify system access and practically limit file access. My hope for our program is that it is recognized within our organization as a partner in State Farm's insurance claims processing effort. To be an effective participant, however, our function must be based on a sound and growing program of administrative competence, exposure identification, management support, user awareness, system access control and file access control. While a sizeable HP operation like State Farm must address these components with large user solutions, I feel that the same data security foundation can be developed by organizations of all sizes to foster an effective and respected program.