

WHITE PAPER

The State of IBM i Security 2012

Are my Power Systems™ servers running IBM i (aka System i[®], iSeries[®], AS/400[®]) **compliant with government and industry security regulations?**

Is my data secure behind the walls of my Power Systems server?
Are we able to **detect fraud, data theft, and other deceptive behavior?**

How do I secure my system in the **most efficient and economical way?**

If you're a senior executive or IT manager with responsibility for Power Systems running IBM i, then you're already familiar with these security-related questions. In response to these issues, PowerTech surveyed over 120 Power Systems servers (many from Fortune 100 companies) in 2011. The results, and the universal nature of IBM i vulnerabilities, led us to conclude that if you have IBM i systems in your data center, then your organization probably suffers from similar internal control deficiencies.

IBM i security projects often take a back seat to Windows- and UNIX-platform security, either because it is assumed that an IBM i server is already secure, or because the security professionals or auditors are unsure how to assess this system.

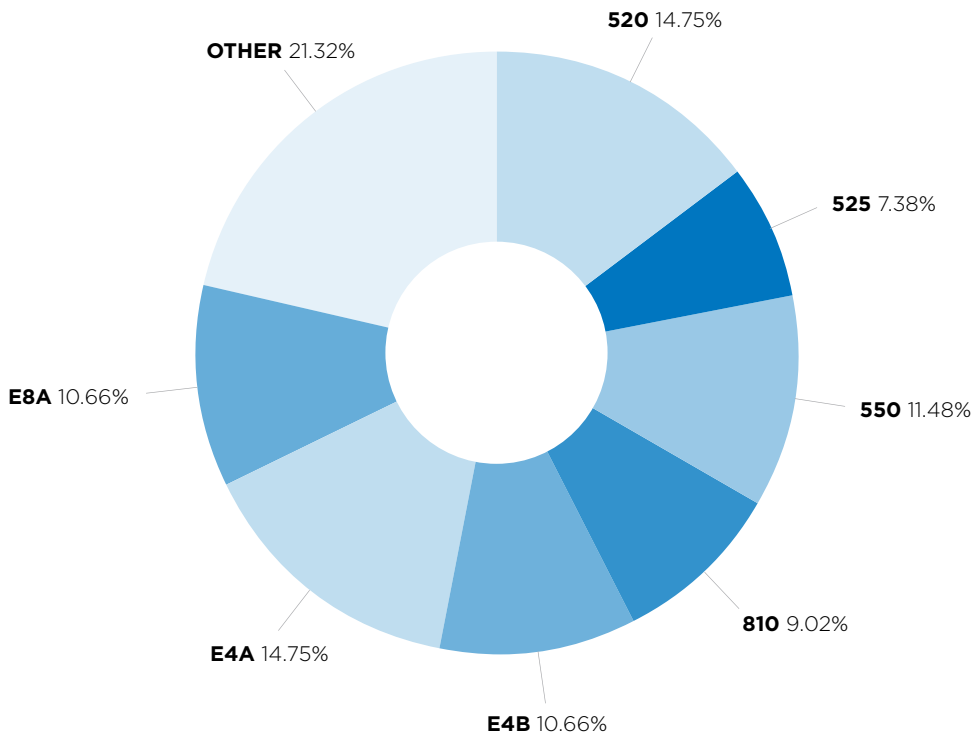
Our goal in releasing this annual study is to help executives, IT managers, system administrators, auditors, and compliance officers understand the important security exposures of IBM i servers and to provide answers to the questions that keep you up at night. >>>

INTRODUCTION: THE IBM i MARKET

IBM introduced the AS/400 in 1988 as its computing system for small- and medium-sized companies. Today, the Power Systems product line ranges from small servers with a single processor to the high-end mainframe-class POWER7 Model 795, which can have up to 256 processors. The IBM i community includes a large and loyal base throughout the world—with more than 380,000 systems estimated in production use. The PowerTech data was collected from a cross-section of systems of varying sizes (**Figure 1**). Companies in industries such as retail, financial, manufacturing, and distribution typically purchased their Power Systems server as part of an integrated business system. Today more than 16,000 banks run their core banking and financial applications on an IBM i server. Many retailers use applications that store credit card data on the system. Some of the more well-known software vendors that provide applications are Oracle (JD Edwards ERP); Lawson/Intentia (financials); FISERVE; SAP; IBM Domino; IBM WebSphere; Jack Henry (core banking); INFOR (BPICS, MAPICS, Infinium, Infor ERP XA applications, PRISM); and Manhattan Associates (supply chain). Given the mission-critical data that is stored on these systems, maintaining a secure configuration should be a top priority.

“Given the mission-critical data that is stored on these systems, maintaining a secure configuration should be a top priority.”

FIGURE 1: SYSTEM MODELS



Over the years, IBM i installations have seen considerable changes in staff. Often, these servers have been running mission-critical business applications for 20 years or more, and the staff that set up server security is no longer there. Consequently, the administration of security controls has lapsed and the guards are down. You'll see that in our results. What you need to consider is, *"Are our guards down, too?"*

METHODS

PowerTech's 2012 Security Study looks at six critical IBM i audit areas:

- **Powerful User Profiles:** Who wields power and who is watching those people?
- **User and Password Management:** Are user IDs and passwords protected?
- **Data Access:** How are individual objects and files protected?
- **Network Access Control and Auditing:** Can unauthorized users reach data through the network and can you detect those activities?
- **System Auditing:** Are you auditing for compliance?
- **System Security Values:** Are you adhering to basic IBM i security recommendations?

For this study, PowerTech reviewed audit and security data from 122 IBM i servers and partitions audited between January and December 2011. This is the ninth year we've conducted this study, which includes results from companies spanning a broad range of industry verticals and company size, including financial, healthcare, communications, education, and transportation. As with previous years, this is not a random sample. The companies in the study were concerned enough about security to request a high-level management audit of their systems. This may have resulted in a sample that is either unusually security-conscious or, at the other extreme, knowingly deficient. Our experience leads us to believe the former is closer to the norm.

The average system covered in the study has 992 users and 493 libraries. These average numbers are a bit higher than the median because there were several larger servers in the data sample (**Table 1**).

TABLE 1: AVERAGE SYSTEM SIZE

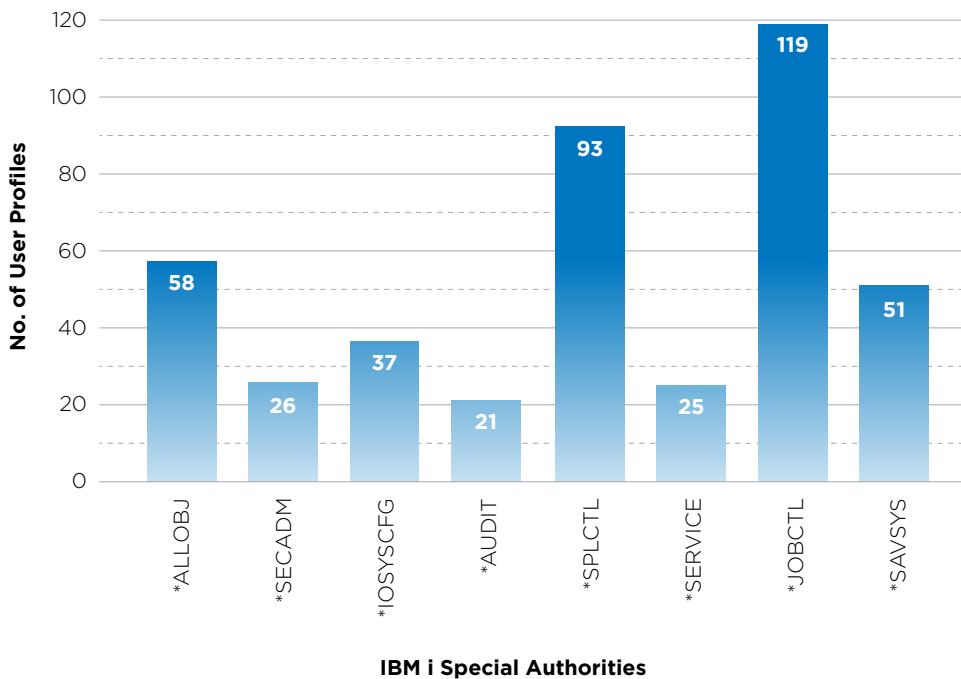
System Size	Average	Median
# of Users	992	410
# of Libraries	493	272

POWERFUL USERS

IT professionals need special authorities to manage systems. In addition to changing system configuration, these authorities include the ability to view or change financial applications, customer credit card data, and confidential employee files. In careless, misguided, or malicious hands, these special authorities can cause serious damage. Because of the risk, auditors require you to limit the users who have these special authorities and carefully monitor and audit their use.

There are eight types of special authority in IBM i (i5/OS, OS/400). **Figure 2** shows the average number of user profiles for each special authority.

FIGURE 2: POWERFUL USERS (SPECIAL AUTHORITIES)



Of all of the special authorities, one provides the user with the unrestricted ability to view, change, and delete every file and program on the system. As shown in Figure 2, this all-powerful authority (*ALLOBJ authority) is granted to users in unacceptably high numbers.

While it is difficult to create a hard and fast rule for all environments, experts agree that the number of users with this special authority should be kept to the barest minimum. As a rule of thumb, we assume it's good security practice to have no more than 10 users with this special authority on any system. Only 7 of the systems reviewed had 10 or fewer users with *ALLOBJ authority.

“In general, the servers reviewed in this sample have too many users that are too powerful. In the hands of careless or disgruntled employees, this could result in data loss, theft, or damage.”

Control Defect: In general, the IBM i servers reviewed in this sample have too many users that are too powerful. In the hands of careless or disgruntled employees, this could result in data loss, theft, or damage. Auditors check for the abuse of special authorities as part of any standard IBM i audit. Even auditors who are not very familiar with the IBM i environment are aware of this issue from their work on other platforms.

Relevant COBIT objectives:

- DS5.3 Identity Management
- DS5.4 User Account Management

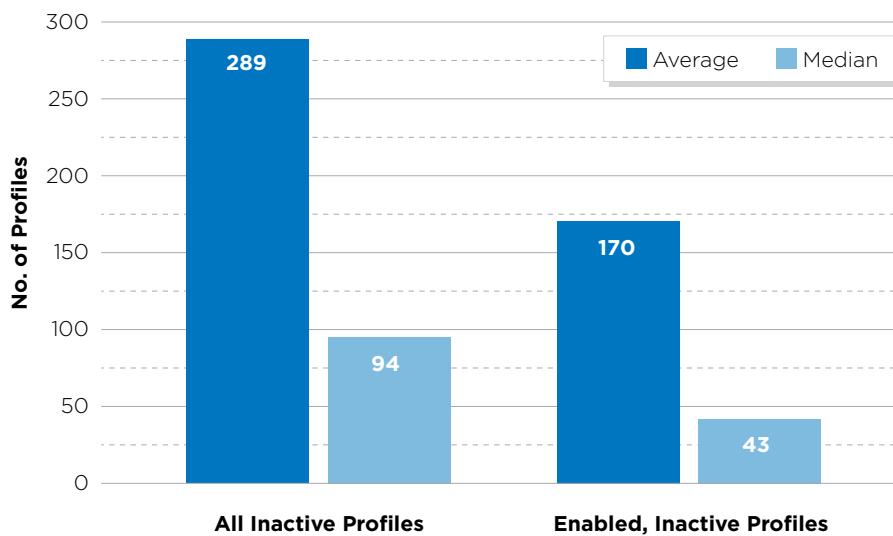
PASSWORD MANAGEMENT AND USER SECURITY

User and password security issues are critical because they represent the most obvious, and easily exploited, method that can be used to compromise your system. Without proper user and password security measures in place, efforts to secure other areas of an IBM i network are largely ineffective because you can't be confident that the user signed on is the same user that the ID and password were assigned to.

Inactive Profiles

In this study, we also looked at the number of inactive profiles—profiles that have not been used in the past 30 days or more. Inactive profiles create a security exposure because these accounts are not actively maintained by their users and are prime targets for hijacking. An average of 170 of the enabled profiles (17% of the total) have not been used to sign on in the past 30 days or more (Figure 3).

FIGURE 3: INACTIVE PROFILES

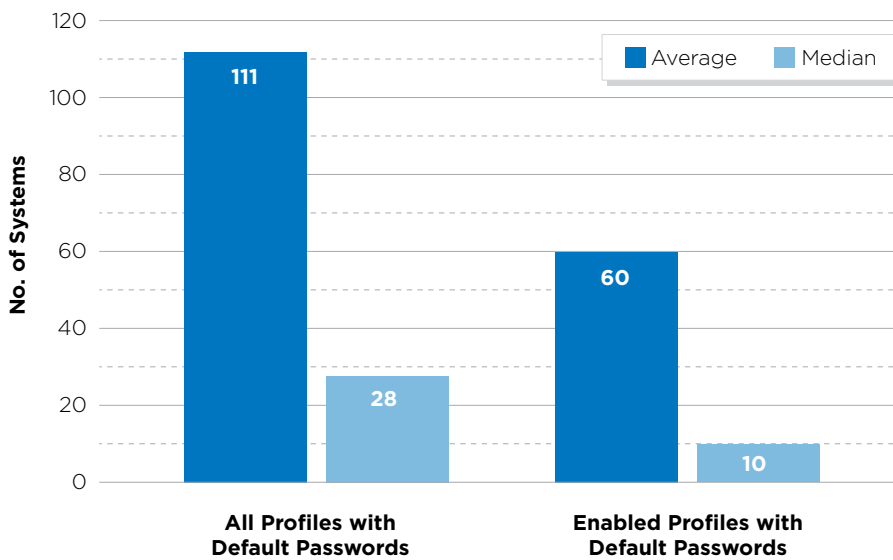


Default Passwords

We also checked for profiles that have a default password (where the password is set to be the same as the username). Because this is the default when new user profiles are created, it is a particularly high-risk factor for IBM i servers. In one interesting statistic in the study, nearly 11% of enabled user profiles have default passwords (Figure 4). Half (49%) the systems in the study have more than 30 user profiles with default passwords (60 out of 122 systems). One system had 3,156 user profiles with default passwords (332 enabled) out of a total of 11,265 users.

“One system had 3,156 user profiles with default passwords out of a total of 11,265 users.”

FIGURE 4: DEFAULT PASSWORDS

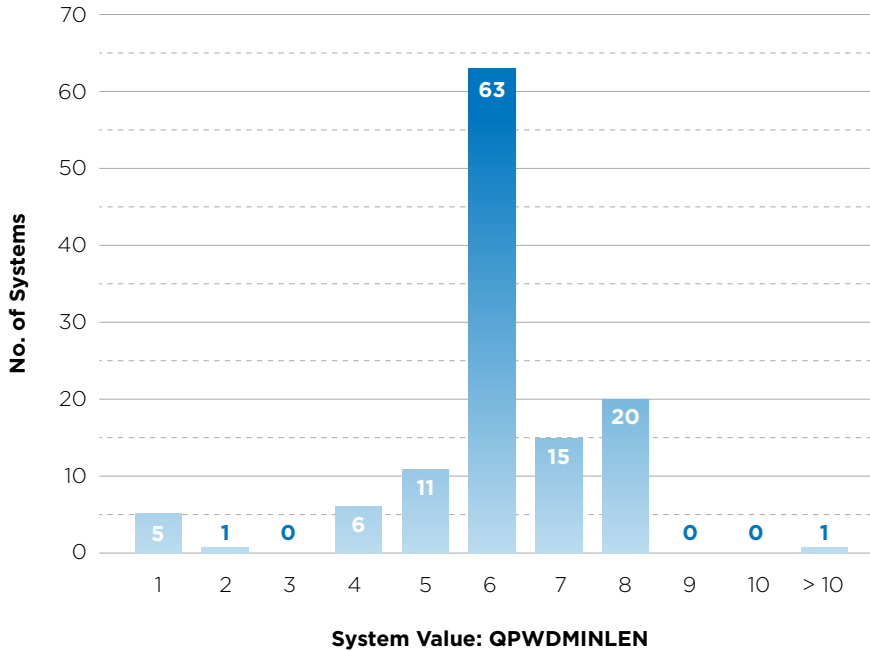


Many companies have policies to name their user accounts or profiles based on a standard format, such as first name initial followed by surname (for example, jsmith, tjones). A hacker, or malicious employee, can guess profile names like jsmith and try default passwords. It’s even easier for an employee who understands the internal standards for user profile names to guess account names and to try default passwords, especially if they are aware of accounts that have been created but not yet used.

Password Length

IBM i provides the capability to require a minimum length for passwords. Shorter passwords may be easier to remember, but they’re also easier for others to guess. Figure 5 shows the setting for the minimum password value on the systems reviewed. Although there are some systems with very low thresholds, the vast majority have the minimum length set to 6 characters or greater.

FIGURE 5: MINIMUM PASSWORD LENGTH



Other Password Settings

Several other features can ensure strict password control on an IBM i server, but system administrators do not always use them. These settings help to make passwords harder to guess, and increase the protection of your system. Some of the more important password settings, and the study findings of their use, are:

- **55%** of systems don't require a digit in passwords.
- **33%** of systems allow passwords to be the same as previous passwords.
- **47%** of systems do not set an expiration time for passwords—users are never forced to change their password.

While good password controls are important, a password expiration policy is equally important. Best practice for a password expiration policy is to set the expiration interval at a maximum of 90 days. According to systems in our study, the average password expiration interval is 78 days. However, 47% of the systems still had their default password expiration interval set to *NONE. If your system is used for accounting or financial reporting, it's best to set an interval for this default system value. Work with your auditors to determine the best policy for your system.

“Overall, the results show that password management procedures are weak and many user IDs are vulnerable to identity theft.”



Invalid Sign On Attempts

Invalid sign on attempts is another area worth closer examination. Many systems in our annual study had several profiles with invalid sign on attempts. It happens to everyone from time to time. Password are forgotten, mistyped, or simply mixed up with other passwords. Help desk personnel charged with resetting these passwords often work with the same users over and over. How do you track which users have multiple invalid sign on attempts? What if your powerful profiles are targeted?

A single invalid attempt, or even a handful of unsuccessful tries, may not be cause for concern. But, what if your system had one user profile with hundreds of invalid sign on attempts? Consider the system in our study with 154,504 attempts. Three, five, or even ten attempts are probably the sign of a frustrated user. Larger numbers could indicate an intrusion attempt. Numbers like 1,000, 15,000, or 700,000 are probably a sign of a broken application that doesn't have a built-in mechanism to identify invalid attempts. The risk level increases significantly if the offending profile is determined to be, for example, QSECOFR, and is not disabled automatically, or if the security team has no way to be notified of failed access attempts in a timely manner.

Control Defect: Overall, the results show that password management procedures are weak and many user IDs are vulnerable to identity theft. Figure 2, Powerful Users, shows that there are an unacceptably high number of powerful user profiles. Consider what could happen if a hacker or a disgruntled employee finds his or her way into an account with *ALLOBJ authority.

Relevant COBIT Objectives:

DS5.3 Identity Management

DS5.4 User Account Management

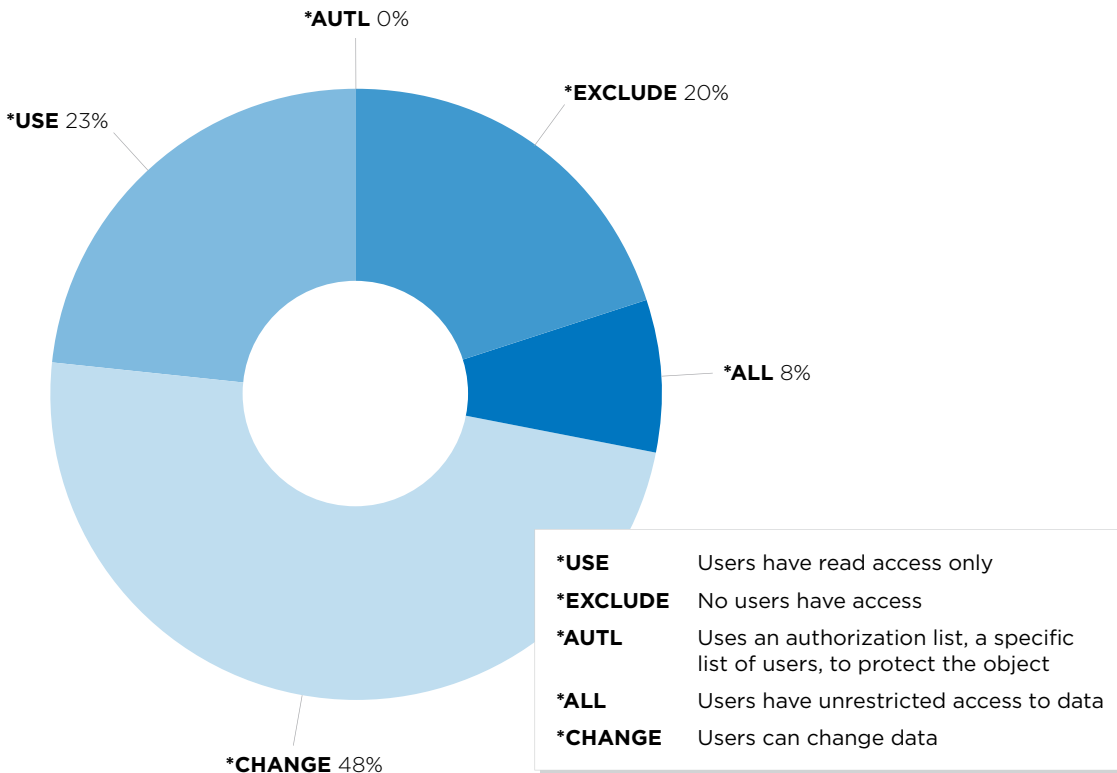
DATA ACCESS

To reduce the risk of unauthorized program changes and database alterations, auditors recommend that the average user (in the IBM i world, the term *PUBLIC is the default indicator for the average user) should not be authorized to read or change production databases and source code. In this study, PowerTech uses the *PUBLIC access rights to libraries as a simple measurement that provides a strong indication of how accessible IBM i data would be to the average end user.

Figure 6 details the level of access that *PUBLIC has to libraries on the systems in our study. If *PUBLIC has at least *USE authority to a library, anyone who can log in to the system can get a catalog of all objects in that library, use or access any object in the library, and even delete objects from the library (assuming that the user or *PUBLIC also has the necessary authority to the specific object). *USE means any user with FTP access can download (read) any data file in the library. The FTP GET function or ODBC operations in tools like Microsoft Excel allow even a novice end user to access your data.

*CHANGE authority to a library allows the user to place new objects in the library and to change some of the library characteristics. Libraries where *PUBLIC has *ALL access allow anyone on the system to manage, rename, specify security for, or even delete the library (if they have delete authority to the objects in the library).

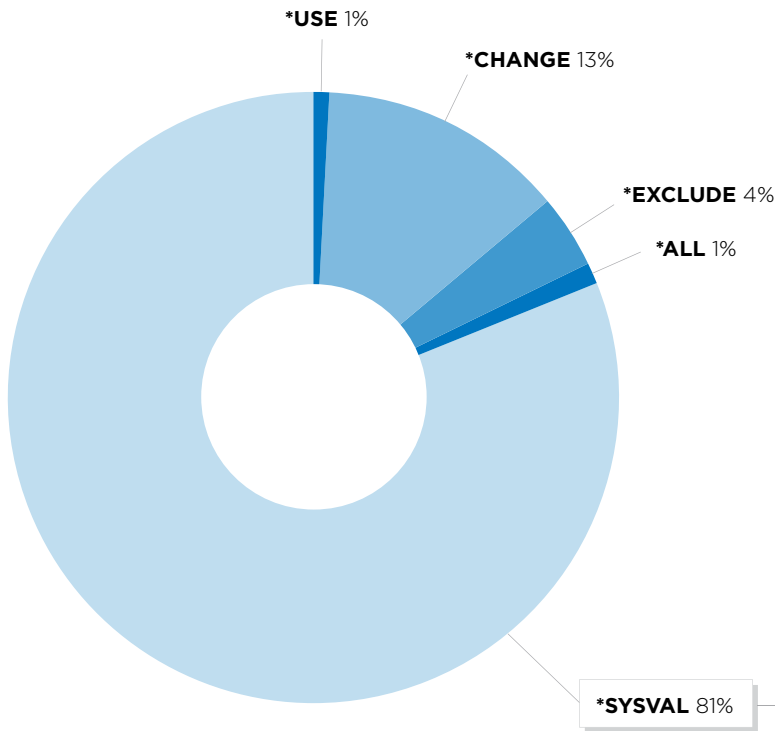
FIGURE 6: *PUBLIC AUTHORITY TO DATA



Our findings demonstrate that IBM i shops continue to have far too many libraries that the average user can access. The statistics for DB2 libraries indicate a lack of adequate control over the data, which often includes critical corporate financial information.

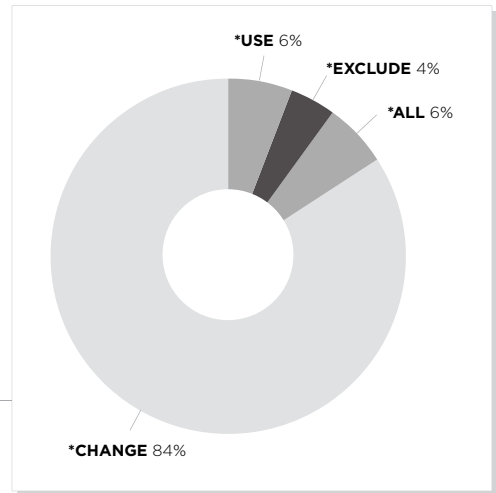
The method used to determine what authority *PUBLIC will have to newly created files and programs typically comes from the library’s Default Create Authority (CRTAUT) parameter. **Figure 7** indicates that 13% of libraries reviewed had Default Create Authority set to *CHANGE or *ALL. However, more than 80% of libraries deferred the setting to the QCRTAUT system value. **Figure 7A** extends the library level assignment of *SYSVAL and reflects that the system value often remains at the shipped default of *CHANGE. In fact, only 4% of systems have been configured to enforce the least-access requirement of common regulatory standards such as PCI. This means that when new files and programs are created on these systems, the average user automatically has change rights to the vast majority of those new objects. On these systems, when anyone creates a new file in one of these libraries, *PUBLIC has the authority to read, add, change, and delete data from the file. *PUBLIC also can copy data from, or upload data to, the file, and even change some of the object characteristics of the file.

FIGURE 7: DEFAULT CREATE AUTHORITY BY LIBRARY



“Overall, these results show that virtually every system user will have access to data far beyond their demonstrated need.”

FIGURE 7A: *SYSVAL PROPERTIES



Control Defect: Overall, these results show that virtually every system user has access to data far beyond their demonstrated need. Auditors typically look to ensure that the company has adequate separation of duties and appropriate controls in place to enforce the separation of duties. This means that the task associated with a business process needs to be distributed among several users. For example, the person who requisitions a purchase order should not have the ability to approve it. Or, the person responsible for security administration and configuration on a system should not be able to approve financial transactions. If object-level authority is not carefully defined, users can circumvent controls and make changes directly to data files. The study indicates that most IBM i shops need to improve their data access controls.

Relevant COBIT Objective: DS5.4 User Account Management

NETWORK ACCESS CONTROL AND AUDITING

Over the years, IBM has extended the power of IBM i by adding tools that allow data to be accessed from other platforms, especially from PCs. Well-known services such as FTP, ODBC, JDBC, and DDM are active and ready to send data across the network as soon as the machine is powered on. Any user who has a profile on the system, and authority to the objects, can access critical corporate data on your Power Systems server.

Even when administrators do not purposely install data access tools on users' PCs, end users can access data using free tools easily downloaded from the Web, or using tools that are included with other software loaded on their PCs. (For example, Windows comes with FTP client software that easily sends or retrieves data from an IBM i server.)

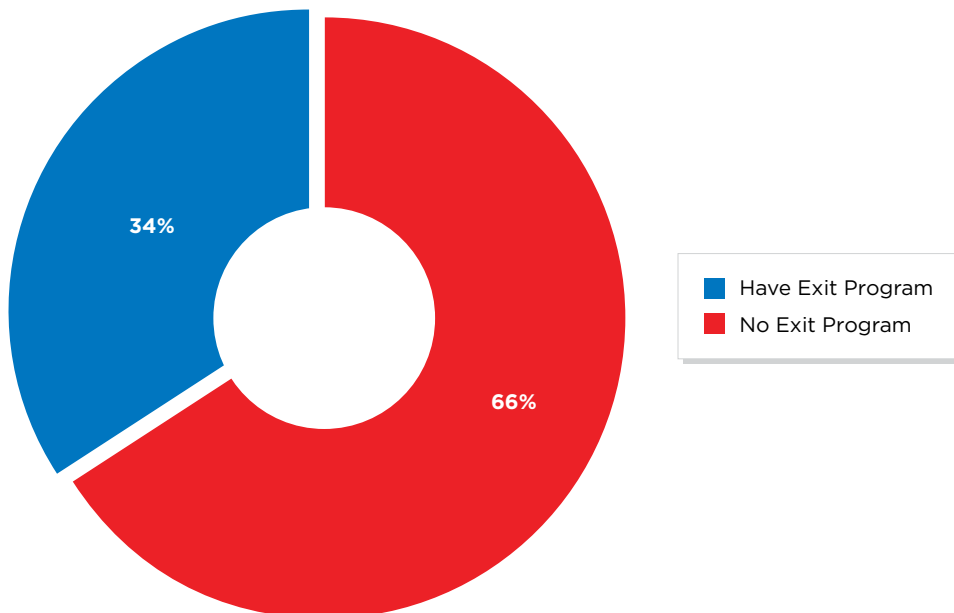
Of course, users can download or manipulate data only if they have the required authority to the objects. However, the results in the Data Access critical audit area indicate that object-level authority is poorly implemented on most systems. The combination of open access rights to data, overly powerful users, and convenient tools to access the data from a PC, is troublesome.

To reduce this serious exposure, IBM provides interfaces known as exit points that allow administrators to secure their systems. An exit program attached to an exit point can monitor and restrict network access to the system. IBM i shops can write their own exit programs or purchase packaged software to accomplish this task. Without exit programs in place, IBM i does not provide any audit trail of user access through common network access tools such as FTP and ODBC.

PowerTech reviewed 27 different network exit point interfaces on each system to check whether an exit program that could provide a security check on the data transfer is registered. Only 34% of the systems in the study had exit programs in place that could potentially log and control network access (**Figure 8**). Even on the systems with exit programs, coverage was often incomplete. Only 22% of the total number of network access exit points were monitored by an exit program.

Of the 34% of systems with exit programs in place, nearly 10% had only 1 exit program, thus not fully protecting their network interfaces. The most common exit point covered was ODBC (for initial connection only), followed by FTP.

FIGURE 8: EXIT PROGRAMS IN PLACE



Users with Command Line Access

Limiting command line access for end users has been the traditional way to control access to sensitive data and powerful commands. In the past, this method was effective. In addition to configuring the user profile with limited capabilities, application menus controlled how users accessed data and when they had access to a command line. However, as IBM opens new interfaces that provide access to data and the opportunity to run remote commands, this approach isn't as sound as it used to be.

Several network interfaces do not acknowledge the command line limitations configured in a user profile and must be controlled in other ways. According to our 2012 results, 26% of users have command line access through traditional menu-based interfaces. Of those 255 users, we found that 66% of the profiles were enabled. This means that system administrators have purposely taken precautions to restrict 83% of their enabled users from using a command line. But now, through network interfaces, these users can run commands remotely, circumventing this intentional restriction.

Control Defect: Based on the broad *PUBLIC authority demonstrated in the Data Access critical audit area, anyone on these systems can access data, commands, and programs without the operating system keeping a record.

Even companies that have installed exit program solutions to protect their data frequently neglect some of the critical access points. It appears that many companies in the IBM i community are dangerously unaware of the wide-open network access problem. The lack of monitoring and control of network access is a serious deficiency in many shops.

Relevant COBIT Objectives:

- DS5.4 User Account Management
- DS5.5 Security Testing, Surveillance, and Monitoring

“Based on the broad *PUBLIC authority demonstrated in the Data Access critical audit area, anyone on these systems can access data, commands, and programs without the operating system keeping any record.”

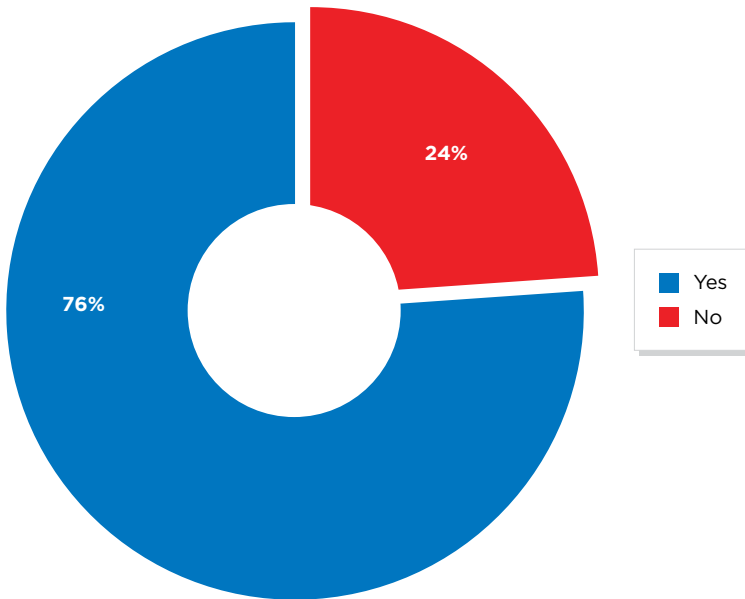
SYSTEM AUDITING

One of the significant security features of IBM i is its ability to log important security-related events in a secure audit journal that cannot be altered. About 24% of the systems reviewed were not using the audit journal (**Figure 9**). Those systems are unable to review recent history to determine things such as “Who deleted this file?” or “Who gave this user *ALLOBJ authority?” The absence of the IBM Security Audit Journal indicates a very low level of scrutiny for the system in question.

When the Security Audit Journal is activated, the volume of data it contains is often so large, and the contents of the log are so cryptic, most IT staff have trouble monitoring the logged activity with the tools available in the operating system. A few software vendors provide auditing tools that report on and review the system data that’s written to the Security Audit Journal. But, only 20% of the systems in the PowerTech study had a recognizable tool installed.

Companies today are overwhelmed by the amount of reporting required to demonstrate compliance with regulations such as Sarbanes-Oxley (SOX) and the Payment Card Industry’s DSS standard, yet it appears that very few of them take advantage of the tools that are available to automate and simplify reporting tasks.

FIGURE 9: SYSTEMS USING THE IBM I AUDIT JOURNAL



“Given the voluminous amounts of raw data that is created by the IBM Security Audit Journal, it’s not realistic to expect system administrators to manually review the logs regularly.”

Control Defect: On most of the systems surveyed, security violations could occur undetected. Companies that use the Security Audit Journal are in a far better position than those that don’t because, at any time, they can use an automated tool to sift through and interpret the audit journal entries. Given the voluminous amounts of raw data that is collected in the IBM Security Audit Journal, it’s not realistic to expect system administrators to manually review the logs regularly. The job of filtering and analyzing massive amounts of complex raw data requires software tools. A software auditing tool reduces the costs associated with compliance reporting and increases the likelihood that this work will get done.

Relevant COBIT objectives:

DS5.5 Security Testing, Surveillance, and Monitoring

SYSTEM SECURITY

Power Systems servers can be configured at a number of different security levels represented by the system value QSECURITY:

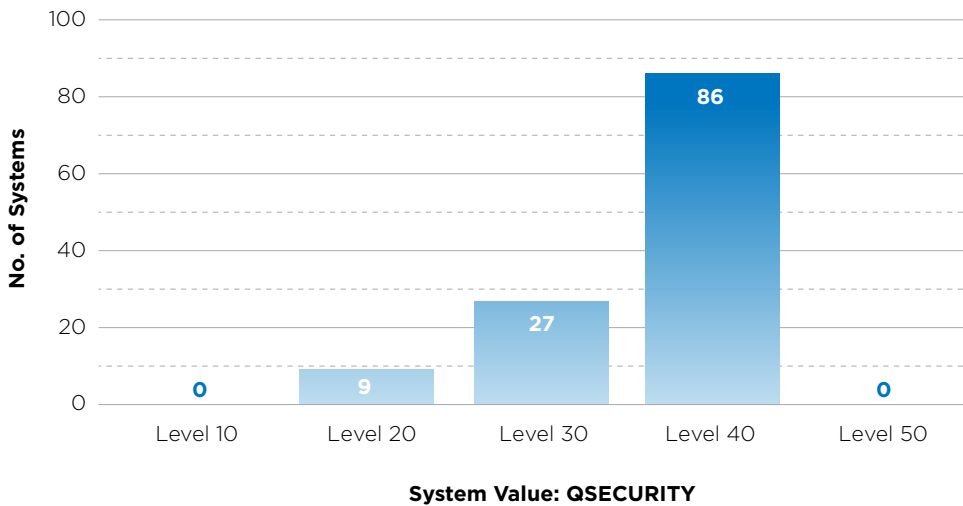
- Level 10** No Security. No password required. User IDs are created for any user who attempts to sign on. IBM no longer supports level 10, and no instances of level 10 were found in this study.

- Level 20** Password Security. Every user must have a valid ID and password. Every user with a valid ID and password assumes root-level authority by default.
- Level 30** Resource Security. Object-level authority is enforced as users do not assume root-level authority by default. A moderately knowledgeable programmer or operator can bypass resource-level security and assume root-level authority.
- Level 40** Operating System Security. Level 30 protection plus operating system integrity. It is possible for an extremely knowledgeable programmer with access to your system to elevate his or her level of authority, possibly as high as root-level authority.
- Level 50** Enhanced Operating System Security. Level 40 protection plus enhanced operating system integrity. A properly secured system at security level 50 is the best defense available. However, even at Level 50, other system configuration issues must be addressed to have a secure system.

“Approximately one-third of the systems surveyed are not following the best practice for overall system security as recommended by IBM and all independent experts.”

Figure 10 shows the distribution of security settings on the systems. Out of the 122 systems in the PowerTech dataset, 29% were running system security level 30 or lower. IBM recommends that this setting should be at level 40 or higher because there are several well-known exposures at security level 30.

FIGURE 10: SYSTEM SECURITY LEVEL



Control Defect: Approximately one-third of the systems surveyed are not following the best practice for overall system security as recommended by IBM and all independent experts.

Relevant COBIT Objectives:
PO2.3 Data Classification Scheme

CONCLUSION

IBM Power Systems have long been perceived as one of the most secure platforms available. But, experts agree that security is only as effective as the policies, procedures, and configurations put in place to manage a system. This study highlights a number of common security exposures and configuration management practices that must be addressed to protect the data on IBM i systems. In general, the study demonstrated that all organizations could improve the IT controls on their IBM i server. In particular, there are six critical audit areas of concern that warrant immediate inspection and action.

Powerful User Profiles

The control defect most readily recognized by both executives and IT professionals is the unbridled and unmonitored power that some IT professionals have over system applications and data. Auditors routinely cite this lack of control when auditing for separation of duties in IBM i shops.

Recommendations:

- Document and enforce “separation of duties” for powerful users. Avoid having any one user being all-powerful, all the time.
- Monitor, log, and report on the use of powerful authorities. Be prepared to justify the use of powerful authorities to auditors and managers.
- Implement a solution, such as **PowerTech Authority Broker**, to automatically monitor, control, and audit users who need access to higher levels of authority. Authority Broker brings an important security capability to IBM i that has long been available to UNIX system administrators.
- Monitor and secure the use of sensitive commands. **PowerTech Command Security** can prevent unauthorized users from executing a monitored command.

User and Password Management

The integrity of user IDs and passwords is a critical component of secure system access. Experienced system managers know that a little bit of attention here can go a long way toward keeping systems secure.

Recommendations:

- Review user accounts on a regular basis to assure that each user’s access is appropriate to their job responsibilities. Automating this step is essential if it is to become a regular part of operations. **PowerTech Compliance Monitor** makes it easy to generate audit reports on a regular basis that compare IBM i user and password information against policy.
- Use a profile management solution to maintain consistency of your user profiles across systems. **PowerTech PowerAdmin** uses a template-based approach to manage user profiles from a central management system.



- Establish and enforce password policies that make it difficult to compromise a user's account.
- Use IBM i system values that make passwords more difficult to guess.
- Eliminate passwords entirely by implementing a Single Sign-On solution based on the Enterprise Identity Mapping (EIM) technology that is included in the operating system.

Data Access

System managers require better processes and tools to monitor and control access to IBM i data.

Recommendations:

- Use the security capabilities of the operating system (IBM i). Where possible, secure data using resource-level security to protect individual application and data objects.
- When it is not possible, or practical, to protect data with resource-level security, use exit program technology to regulate access to the data. **PowerTech Network Security** is the industry's leading off-the-shelf exit program solution.
- Monitor changes to your database information. **PowerTech DataThread** creates before-and-after snapshots of database changes and requires users to sign for changes, so you can meet compliance requirements.
- Investigate how well your third-party software suppliers use operating system resource-level security. Seek assistance from the vendor in protecting application objects.
- Ensure that application libraries are secured from general users on the system. (Set the System Value and Library values for Default Create Authority to the most restrictive setting [*EXCLUDE].)

Network Access Control and Auditing

This is not being addressed in most IBM i shops, so both authorized and unauthorized access occurs without accountability or traceability. IBM's exit point technology provides the ability to control and monitor network data access. However, the study indicates that the adoption rate of exit points has not kept pace with the adoption rate of network data access utilities.

Recommendations:

- Implement exit programs using **PowerTech Network Security** to monitor and control users' access through network interfaces such as ODBC and FTP.
- Review network data access transactions for inappropriate or dangerous activity.
- Establish clear guidelines for file download and file sharing permissions.
- Remove default DB2 access in tools like Microsoft Excel and IBM i Client Access.

System Auditing

Given the volume of security-related transactions that occur on a system in a typical day, tools are essential to quickly find the information that deserves your attention.

Recommendations:

- Every IBM i shop should use the IBM-supplied Security Audit Journal (QAUDJRN) to ensure that important events are recorded in a non-alterable log.
- Implement **PowerTech Compliance Monitor** to simplify the task of reviewing audit logs for relevant events such as object deletions, user ID promotions, and system value changes.
- Implement **PowerTech Interact** to include IBM i security data into your Enterprise Security Solutions that support Security Information and Event Management (SIEM) or Syslog formats.

System Security Values

System values regulate how easy or difficult it is for an outsider to use or abuse your system. Poorly configured or unmonitored system values are an unacceptable security risk. Organizations that are unsure of the potential impact may want to consult with IBM i security professionals before making changes, but a solution should be applied quickly.

Recommendations:

- Define and implement a security policy that incorporates the most secure settings your environment will tolerate. (Seek professional expertise if you are unsure of the impact of certain settings.) Download PowerTech's free Open Source Security Policy to help you get started defining your own policy.
- Run the System Values reports and scorecards in **PowerTech Compliance Monitor** on a regular basis to ensure that your system settings match your policy.

Appendix I: COBIT

Organizations that start security projects usually find out early that legislation is vague when it comes to IT security issues. Legislations seldom give specific actionable recommendations, and never mention specific platforms like Power Systems running IBM i. So, where should you start to look when evaluating your business-critical servers? For SOX, the U.S. Securities and Exchange Commission (SEC) has ruled that management must evaluate the company's internal controls over financial reporting using an acceptable, recognized control framework. This requirement for frameworks also applies to the Information Technology (IT) arms of the organization. Some of the best known standards are COBIT, ISO 27002, and ITIL.

While there is no "golden standard," most large audit firms now use COBIT as a generally accepted standard for IT security and internal control practices. Several of the COBIT objectives that are relevant to security compliance on IBM i servers are outlined on the following page:



DS5.3 Identity Management

Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository.

Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management

Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance, and Monitoring

Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.








PO2.3 Data Classification Scheme

Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme includes details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving, or encryption.

Appendix II: PowerTech Solutions

As the leading expert in IBM i security, PowerTech has developed an extensive line of powerful solutions designed to address shortcomings in the operating system, provide advanced functionality in access control and auditing, and ease the cost and burden of maintaining regulatory compliance. **Table 2** outlines the available security modules and their purpose.

TABLE 2: POWERTECH'S COMPREHENSIVE SUITE OF SECURITY SOLUTIONS

 Compliance Monitor	Custom auditing and reporting
 Network Security	Access control by exit programs
 Authority Broker	Management of privileged users
 Interact	Real-time security reporting
 DataThread	Real-time database monitoring
 Command Security	Command monitoring and control
 PowerAdmin	Centralized user profile management

ABOUT THE STUDY AUTHORS

PowerTech is the leading expert in automated security solutions for IBM Power Systems servers, helping users manage today's compliance regulations and data privacy threats. Our security solutions are designed to save your valuable IT resources, giving you ongoing protection and peace of mind.

Because Power Systems servers often host particularly sensitive corporate data, organizations need to practice proactive compliance security. As an IBM Advanced Business Partner with over 1,000 customers worldwide, PowerTech understands corporate vulnerability and the risks associated with data privacy and access control. PowerTech security solutions are the corporate standard for IBM i security at many major international financial institutions. PowerTech is a Help/Systems, LLC company and maintains its corporate headquarters in Eden Prairie, Minnesota.

Founded in 1996 by security experts, PowerTech has demonstrated a proven commitment to the security and compliance market and leads the industry in raising awareness of IBM i security issues and solutions.

- PowerTech is a member of the PCI Security Standards Council, a global open standards body providing guidance to the Payment Card Industry (PCI) Data Standard. PowerTech works with the council to evolve the PCI Data Security Standard (DSS) and other payment and data protection standards.
- PowerTech is a member of the IBM i Independent Software Vendor (ISV) council.
- PowerTech publishes many educational white papers, including the IBM i Security Study. First published in 2004, more than 1,500 systems have been assessed to date.
- PowerTech publishes an Open Source Security Policy for IBM i as a part of its mission to promote awareness of common security challenges and ensure the integrity and confidentiality of IBM i data.

