Batten Down the Hatches™

Plugging the vanilla BPCS security leak

The problem with standard BPCS security

Any iSeries software package has these two security components:

- OS/400 object security **external** to the package
- **Internal** security provided for by the package itself

Using BPCS internal security, authority can be granted to specific programs. INV100 – Item Master Maintenance is a good example. However, for INV100 to work correctly, user access to all of the objects used by Item Master Maintenance (programs, display files, print files, data files, etc.) must be granted externally by i5 operating system security. Without that externally-granted access, the BPCS program won't work.

Vanilla BPCS versions 6 and earlier solve the operating system access requirement by employing a group profile. All BPCS users are part of the group profile 'SSA' and that profile owns all BPCS files and objects. Since all members of a group profile have the same OS/400 security rights as the group profile itself, that means that all BPCS users have ownership rights to all BPCS objects and files.

When users are operating within the boundaries of the BPCS product, that's acceptable because internal BPCS security controls what parts of BPCS the user has authority to. However, a user can access BPCS objects from outside the scope of BPCS security. It can be done off the command line in 5250 emulation or from a personal computer (via FTP, Operations Navigator, etc.).

The implications

It's an enormous security risk. Vanilla BPCS security opens the door for accidental or intentional catastrophe. Here are three illustrations:

- The vanilla BPCS design permits user X to change the list price for an item by using DFU or SQL even though the BPCS security officer has configured internal BPCS security with the specific intent of prohibiting user X from changing anything about the item master.
- Furthermore, if BPCS user X has authority to write Queries, user X could accidentally clear all data in the item master file by simply typing the wrong file/library name in the Query definition.
- A BPCS user who wants to do something unconstructive could choose to delete the month-end programs or the entire General Ledger.

Over and above the risks described, any BPCS user who happens to have command line access can invent accidents and catastrophes from within the BPCS product.

The not-so-great solution from INFOR

INFOR acknowledges the problem and has a solution which is very time consuming and very expensive. They have several BMRs to solve it for BPCS versions 6 and earlier.

Here's a high-level look at the **time consuming part** of the INFOR approach:

The BMRs change a few programs to address this issue from within the BPCS product.

Installing BMRs is only the beginning of the fix, however. INFOR also provides a white paper which explains all of the manual changes that must be executed for every BPCS object and data file. Each OS/400 user profile also requires manual adjustment. It's takes a very considerable effort over a number of weeks to do all this work.

Here's a look at the **expensive part** of the INFOR solution:

The BMRs and associated white paper are only available for enterprises that have acquired On-going Support contracts with INFOR. If your company hasn't already paid for OGS support, the solution is not available to you. We continue to hear anguish about the cost of OGS.

Unbeaten Path's 'Batten Down the Hatches' solution

'**Batten Down the Hatches**' is a much less expensive and much less time consuming alternative to INFOR's BMR approach. It is a service performed by Unbeaten Path International for each BPCS environment and all BPCS-related libraries on your iSeries. The key benefits of this service are:

- BPCS access for BPCS users to BPCS objects and data files will still be entirely controlled by BPCS' internal security logic.
- OS/400 access for BPCS users to BPCS objects and data files will be restricted if that access is attempted from outside the BPCS system.

'**Batten Down the Hatches**' addresses i5 operating system access to BPCS data for all standard BPCS programs executed from within BPCS as well as custom programs that access BPCS data from within BPCS.

Our technical staff can explain the facets of operating system security functionality which are utilized to achieve these benefits. The '**Batten Down the Hatches**' service accomplishes the job by running our proprietary software over BPCS objects and data files in each BPCS environment and over each BPCS-related library. There are a very limited number of exceptions which we then address manually.

The process includes communication between Unbeaten Path and the client to identify environments and review exceptions. During these discussions we will also review the default authorities for each user to each environment and either accept or change those authorities.

Testing of the changes before production implementation will be closely coordinated between Unbeaten Path and client staff.

How 'Batten Down the Hatches' addresses exceptions

Security settings generated by **Batten Down the Hatches'** utilities typically prohibit access to BPCS data by applications executed from outside of BPCS. However, our experience has taught us that exceptions to this rule may be required.

We will be able to easily identify some of the exceptions because we have encountered them during prior engagements. It is our hope that project "kick-off" discussions with your technical staff will alert us to many of the other exceptions.

The appropriate security authority for each identified exception will be planned in consultation with your technical staff so as to narrow access without compromising required functionality

If some BPCS users must execute operating system commands, then our **By Invitation Only**® software can be employed to grant one or more specific users access to a limited number of specific commands without giving those users command line access. Click **here** to learn more about By Invitation Only.

Internal control compliance

If Sarbanes–Oxley compliance is a requirement for your enterprise and you haven't already solved this vanilla BPCS security problem, then Batten Down the Hatches is be a natural fit for your enterprise.

> Click **here** to see a sample deliverable Unbeaten Path prepared to help a company that was trying to prepare well for their next external audit.
>
> Click **here** to see an index to other Unbeaten Path products that help cope with third-party internal control requirements.

Questions ?

It would be a privilege to answer any questions about **Batten Down the Hatches** services and software. Here's Unbeaten Path International's contact information:

> **Toll free North America: (888) 874-8008**
> **International: (+USA) 262-681-3151**
> **Send us an e-mail** (click **here**)

Unbeaten Path®