Web and Collaboration Strategies Service

The Business Critical Portal Imperative

Prepared For:	Larry Bowden, IBM
Prepared By:	Craig Roth, Vice President
Delivered On:	January 14, 2003

The State of the Portal

As 2003 begins, it is reassuring to look back and see how far portals have come, but daunting to see how far they have to go before they reach their full potential. Architects have become increasingly aggressive about recognizing redundant functionality across applications and pulling it out into reusable infrastructure. Vendors have assisted with this effort by opening up enterprise applications to better leverage existing infrastructure as well as providing new types of infrastructure on which to build applications. Over the past 2 years, technologies that aid in the delivery of interfaces to end users have seen particularly rapid growth. Technologies such as personalization, device rendering, applying style sheets, single sign-on, and usage tracking, are being pulled out of proprietary applications and reborn as infrastructure so that they can be broadly leveraged across all of an organizations' systems. Furthermore, once a layer of delivery infrastructure is placed above applications, end-user focused integration technologies that integrate applications, content, and collaboration can also be better leveraged. Portal frameworks have emerged as a fulcrum for bringing these delivery technologies together.

Many existing portals are just aimed at one group of users and are often used as an alternate access mechanism rather than something the business relies on. We see two trends that will drive organizations to accept portals as business critical: the ability to meet the needs of users outside the organization's employees and the ability to deliver the availability, maintenance, and security required to support mission critical functions.

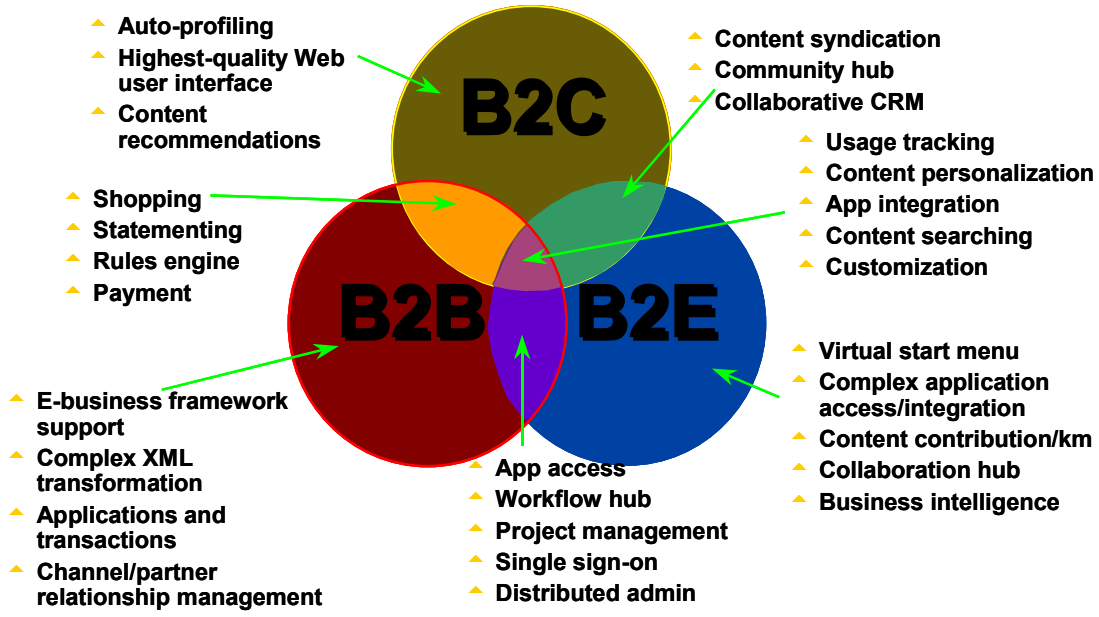
Moving the Portal Beyond the Intranet

2002 brought the first generation of portal products that were ready to support a full range of enterprise portal demands, including multiple content types (documents, applications, databases, collaboration) and internal and external constituencies. However a survey of over 200 respondents conducted by the META Group at our conferences in the first half of 2002 found that most organizations (60%) still concentrated on the internal use of portal technology, instead of using it for partners, suppliers, or customers.

The combination of integration, collaboration, and content management technologies has proven to have significant benefits. META Group case studies have found multi-million dollar net present value to several large employee portal projects with cash flow, productivity, and strategic benefits. The features needed to produce employee (B2E) portals can be seen near the B2E circle in the figure on the next page and are present to some degree in most enterprise portal products. However, to leverage these benefits in the business-to-business (B2B) or business-to-consumer/constituent realms (B2C), new features are emphasized. B2B portals share the need for single sign-on, workflow, and application access with B2E portals, but also require features such as support for popular e-business frameworks and complex XML capabilities. Likewise, B2C portals can benefit from the same community and collaboration features that employees enjoy, but the personalization, profiling, and usage tracking capabilities are much more complex than those needed for employees. A business critical portal will need an expanded set of features to be usable outside the comfort zone of the corporation.

As organizations become comfortable with their employee portals, they will increasingly attempt to stretch them to cover partners and employees. We expect B2B usage (encompassing partner and supplier portals) to expand to 35% by 2004 and 50% by 2006. Customer portals will increase more slowly at first (30% by 2003), but match B2B at 50% by 2006.

Our clients also indicated a preference for using the same product for employee, partner, supplier, and customer portals in order to minimize complexity. Indeed, 78% of the survey respondents intend to use the same product for at least two of these areas. This means that organizations find value in the portal concept and would like to leverage its benefits outside of their company, but they will need a strong product before they feel comfortable using them in this higher stakes arena. They need a portal that can handle business critical systems.



Creating a Reliable, Maintainable, Secure Portal

In addition to having an expanded set of features, organizations building portals to enable business critical collaboration with partners and customers will require the same levels of reliability, maintenance, and security that are found in more mature systems. A system is business critical if fundamental goals of the business will not be met if the system fails. This is a lot of pressure to put on a technology category that is only 4 years old! However, with an experienced vendor and a reliance on enterprise class infrastructure, portals can achieve this goal.

For a portal to be business critical, the following operational imperatives must be addressed:

Reliability

1. *Deliver High Availability*

   Like any other system, guaranteed availability will be demanded of a portal. While it is typically agreed upon in a user-centric service level agreement (SLA), an organization must first ensure the application and underlying infrastructure are architected such that they can support the level requested by business managers. Portal technology is often deployed initially as an alternate mechanism for employees accessing content and applications and can be held to relatively loose uptime standards (i.e., 95-99%), with large maintenance windows. As an organization learns how to manage a portal, this percentage typically increases. An externally facing portal should be held to the same standards as any other external facing Web application, where META Group best practices have identified the need for 99.9% or greater availability, with many organizations nearing 100% availability. No portal should be deployed in a business critical environment until it can support these service levels.

   Availability should be monitored via a robot simulating the end user presence for each type of user (for a bank, the types might be consumer customer, commercial customer, prospective customer, affiliate, etc.). A process for regular review of availability history and incorporation in the organization's monitoring, notification, and escalation systems and processes is essential.

2. *Reliable Integration with other Business Critical Applications*

   Integration points represent obvious points of failure for any business critical system. Even if the portal itself is functioning properly, it needs to ensure that its connections to dependant systems do not break. By definition, any downstream system that a business critical portal depends on is also a business critical system. While a portal cannot control whether a downstream data provider goes down, it can handle such outages gracefully by quickly returning an error or cached data (rather than hanging and causing a bottleneck), alerting support personnel to the issue, and possibly even removing links to the portlet until the issue is resolved.

   XML-based Web services will become more critical in 2003 and especially 2004 as a common integration mechanism across applications and enabling integration through firewalls (useful with partners and suppliers). Any business critical portal will therefore need to have good XML support (ability to easily grab data from XML documents) and web services capabilities (standards support and a development environment for creating portlets out of web services).

3. *Reliable Supporting Infrastructure*

   A portal can only be as reliable as the infrastructure that supports it. Infrastructure components leveraged by the portal (e.g., directory, application server, network) need to have load balanced, clustered, redundant capabilities and procedures need to be in

place for monitoring of the external infrastructure services that are necessary for the proper operation of the portal. This will take different forms depending on the service that will be monitored, from a ping of the service to detailed performance monitoring with a local resident monitoring agent. This data will be also be used for service level reporting.

Most organizations will choose to have a management console that consolidates the data from the many monitoring tools, agents, locations to a single screen representin the health and performance of the portal as a whole. This will provide an "application" view, which is necessary to identify when portal level problems arise, not just infrastructure or application component issues.

4. *Rapid Response Time*

A business critical portal must have the ability to perform well under heavy loads. Any SLA conforming to best practices will identify application response times users must receive for key functions within the portal. More advanced organizations will take the next step and identify differentiated response time based on peak usage times, peak usage loads, and business critical cycles (e.g., a portal that may be more heavily used during tax season will have a tax season SLA specified). This implies that not only is the portal architect properly, but proper response time monitoring is in place. The monitoring must act as an early warning system identifying when the response begins to degrade, not that it has significantly degraded.

Properly deploying the application dictates that testing tools and scripts will be necessary for load and functional testing prior to the portal's release. A subset of the scripts should be leveraged for operational monitoring while running in production. The ability to stress test individual portlets may be necessary in a portal that is expected to get heavy loads. If a test environment cannot mirror the production environment, plan to run periodic off hour tests against the true production system, ensuring load handling and key functional abilities.

5. *Debugging/root cause tools*

To solve problems and prevent them from recurring, a portal will need to provide a mechanism for debugging its operation or determining the root cause of failures. The main areas to be debugged are personalization rules and portlets. This will require not only the monitoring of the infrastructure the portal and its components run on, but also each individual element necessary to support the portal. The relationship between these elements (e.g., which application is tied to each portlet) must be maintained. This configuration management is the key to speeding any root cause process.

6. *Expected Behavior*

Any business critical application must not only be present but must behave as expected. This is beyond just having all the infrastructure and application components present or having them respond within the proper time. It is about reliability of response. Is the portal acting as it is expected? Does it return the proper

data? This can be accomplished via robots executing against the application or watching actual end user traffic (e.g., active or passive monitoring), leveraging response time monitoring infrastructure. 20%+ of the reported application problems are due to an application not returning the proper data, or not behaving properly, though it may have responded within the predefined levels. Failure to monitor this with business critical portals will lead to not only unhappy users, but missed opportunity, as users have proven they will avoid technology that does not behave properly.

Maintenance

7. *Back-up and recovery*

   Over time, a portal accumulates a significant amount of metadata about its users, content, configuration, and applications that could be very time consuming to recreate in the event of a catastrophe. For this reason, a portal must not just have the data backed up, but also its critical metadata including elements such as user profiles, personalization rules, content metadata (taxonomy and classification), access control lists, portal layouts, style sheets, and portlets. For better availability hot back up or load balanced architectures can be used. Also, a recovery plan must be in place that supports recovery of individual elements or the entire portal.

8. *Automated change and configuration management*

   As with any other software, portal vendors often roll out new versions and patches to their software. When multiple instances of a framework's code exist in server farms, across divisions, or inside/outside the firewall, it becomes necessary to have an automated change and configuration management environment. While a centralized administration capability should cover changes to portal elements such as portlets, style sheets, and access control lists, a configuration management system may be required to distribute changes to the portal code itself. Failure to automate this process will not only increase support costs, but will also lead to more downtime, as manual change is the largest cause of outages, due to errors made during the complex process. Automating can be as narrow as automation of the installation/distribution of production code onto the servers or as broad as automation of the entire process from the time development states they are code complete (e.g., interfacing with QA environment, code movement). Additionally, organizations cannot forget to track the configuration of the underlying infrastructure and ensure that these infrastructure components can support the new releases of the portal (e.g., can this version of the OS support the portal software that will be installed on it or does it require a patch).

9. *Centralized Administration*

   A portal framework provides the capability to build multiple portals to fit the needs of different constituencies. There may be a sales portal, HR portal, portals for different departments/divisions, or for different customer types. But they all leverage the same infrastructure and often similar capabilities from the framework. This means that for a complex organization with dozens of portal servers, there needs to be a mechanism for rolling out changes to elements that may be copied on multiple servers such as portlets, security policies, style sheets, roles as well as a mechanism to lock down

elements that individual portal owners cannot change. While utilities to support this administration may vary based on underlying hardware, development environment, or geography, the operational processes must be the same, ensuring consistency – particularly in change and configuration management.

10. Workflow for all critical parameters

Making a mistake in a personalization rule or deploying a new portlet before it is ready generally have minimal impact in employee-centric, departmental portals. But sending the wrong message to a customer can be disastrous. Therefore, a business critical portal will need to support levels of workflow and approval for changes to parameters affecting the end user. This includes style sheet modifications, personalization rule changes, access control lists, and deployment of new portlets or content.

Security

11. Enterprise Class Security

While employee portals can have complex security demands (particularly for remote VPN access), the difficulty of ensuring security when systems are opened up to partners and customers is even greater. Simple web sites with no application access and minimal confidential data can simply be placed in a DMZ and disconnected from any critical internal systems. However, this kind of simple "brochure-ware" site also yields minimal benefits. For portals to automate customer and partner processes, increase satisfaction, and reduce administrative overhead they need to connect external users to applications and help them communicate with employees. A business critical portal therefore requires more complete security infrastructure processes that secures the information in the portal as well as the portal itself. This higher level of security will require the portal and the identity infrastructure around it to provide:

- Ability to work through outbound and reverse proxies to hide the applications being presented by the portal from direct access.
- Ability to cooperate with (act as a proxy for) authentication mechanisms that use technologies such as HTTP and SSL to validate user credentials.
- Ability to work with authorization mechanisms and synchronize directory information with existing user repositories.
- Use of secure, encrypted communication lines, from the portal out to the user (selective use of HTTPS to avoid performance bottlenecks) and from the portal to back end systems (using technologies like SSL or IPSec)
- Access control capabilities for the administrator that permit granting or revoking granular (i.e., individual pieces of content, specific discussion groups) or broad access rights to individual users and groups of users.
- Audit trails of failed access attempts and portal activity.

Conclusion

Portals need to move beyond being just an "intranet on steroids" to reach their full potential and yield maximum benefit to the organization's bottom line. In order to leverage its capabilities for suppliers, partners, and customers, organizations, portal owners will need to:

- Gain confidence in the reliability, administration, performance, and security of their portal framework internally before using it in business critical situations
- Select a portal that provides the functionality needed by external constituencies as well as internal
- Ensure that the processes and technology are in place to support a portal as a business critical system, including service level agreements, backup/recovery procedures, enterprise-scale monitoring and alerting, and comprehensive security

Once these needs are met, an organization can realize greatly increased benefits from their portal frameworks such as cost reduction, improved customer service, and quicker reaction time to changes in the business environment.