e-government infrastructure
September 2001

Creating an infrastructure for e-government: enabling government innovation

e-government strategy and solutions team
IBM Public Sector

Introduction

…e-government is applying e-business to the transformation of government and governance

Few technologies have revolutionized business more than the advent of the Internet. Since the mid-nineties, organizations all over the world have come to realize that the Internet’s true value is not in people’s ability to browse the Web or send e-mail, but rather, in the new opportunities it creates for enhancing business processes, reducing costs and delivering better services.

e-government is the application of e-business to government. It is not simply defined as e-commerce transactions; it is about using technology to redefine organizational models in order to extend relevance and maximize value. It is the realm of technology-enabled transformation.

With the evolution of e-business technology, non e-government models and organizational structures will be faced with increasing pressures. People used to say that government had no competitors, but that was clearly wrong. Government’s competitors exist in the shape of other governments and jurisdictions, intermediaries, private sector providers, etc.

The infrastructure of e-business has become a mission-critical component… that cannot be overlooked…the risk of infrastructure problems continues to grow.

Aberdeen Group

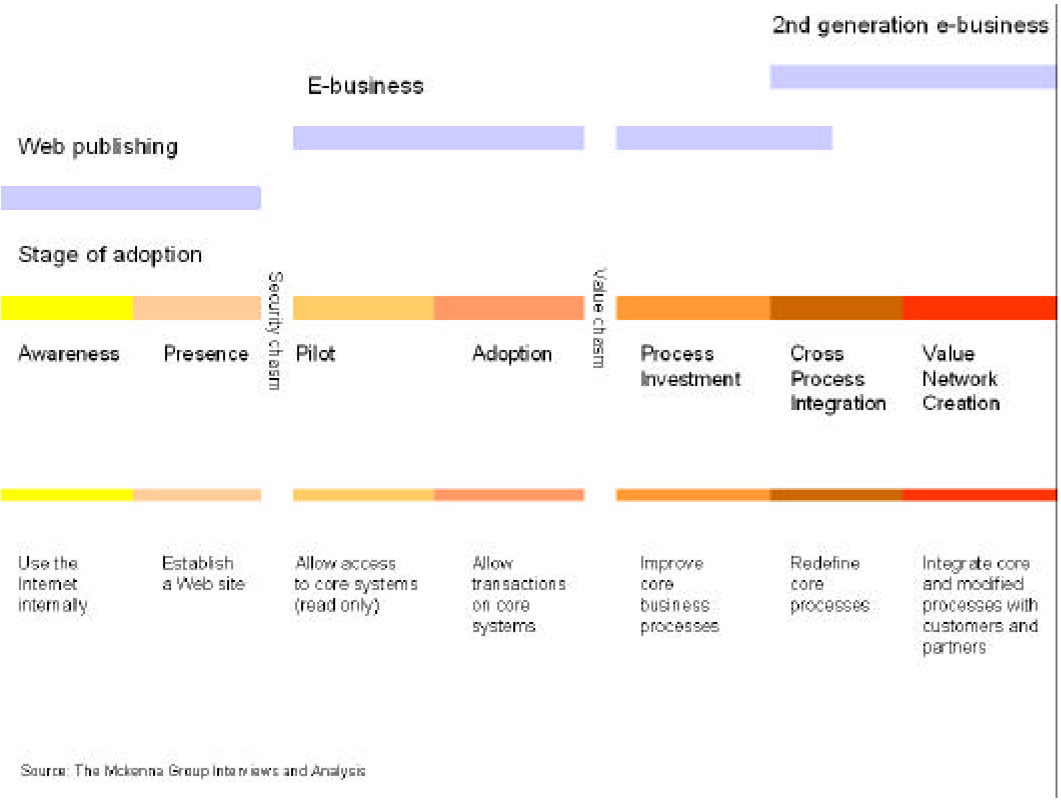
These competitors will exploit new technologies as much as possible. New business models are emerging, along with enhanced constituent experiences, which offer alternatives and weaken a particular government’s “mind share”. In order to compete in this new era, governments at all levels must be able to react quickly to challenges - constantly innovating their processes to stay relevant in meeting public service expectations and priorities.

To accomplish this, it is becoming imperative for government organisations to build technical infrastructures flexible enough to absorb new technologies quickly, and rapidly to alter the scope and function of applications to support changes in the government business model.

This document investigates the requirements e-government places on Information Technology (IT) infrastructures, and provides guidelines for creating an infrastructure that offers the flexibility and reliability necessary to support the constant evolution of processes in the e-government world.

The Evolution of e-Government

A research study by The McKenna Group shows four major phases enterprises go through as they become more involved with e-business:


2nd generation e-business
E-business
Web publishing
Stage of adoption
Security chasm
Value chasm
Awareness
Presence
Pilot
Adoption
Process Investment
Cross Process Integration
Value Network Creation
Use the Internet internally
Establish a Web site
Allow access to core systems (read only)
Allow transactions on core systems
Improve core business processes
Redefine core processes
Integrate core and modified processes with customers and partners

Source: The Mckenna Group Interviews and Analysis

Figure 1: e-business adoption process

We see these phases exactly paralleled in the development of e-government.

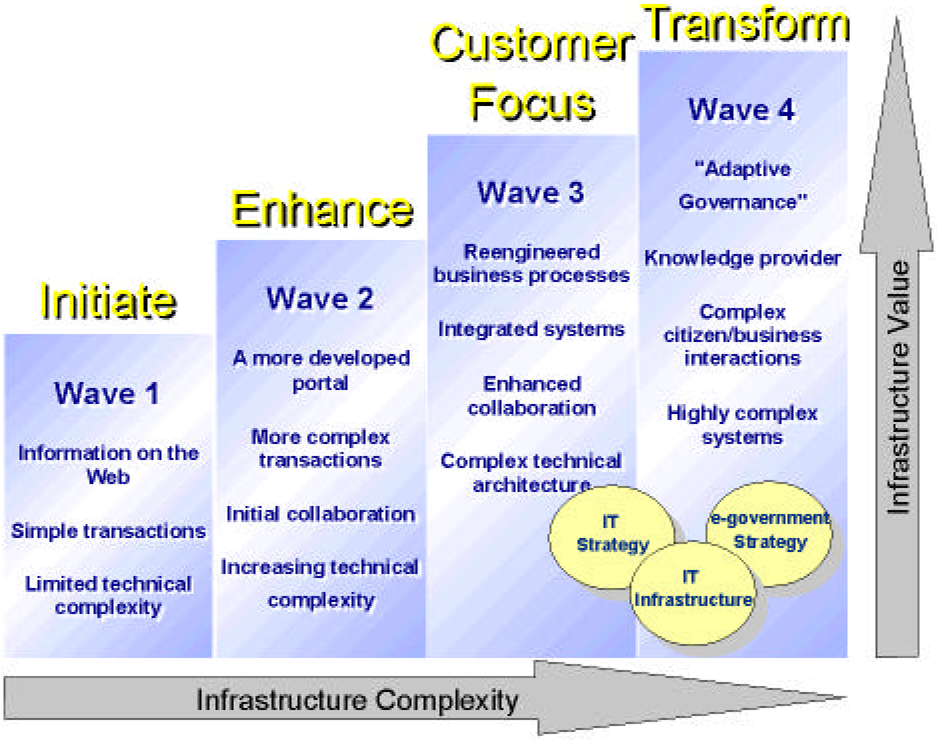


Figure 2: evolution of e-government

The next critical phase will be an increasing focus on becoming "customer-centric". Technology-enabled transformation is the key to reaching new ways of interacting with constituents, rather than replicating online the existing structures and process of government.

- **Wave 1** is where most governments began their transition to e-government. Governments at all levels were keen to publish information about themselves and their services on the Web. They used the Internet as simply another way of reaching constituents with information. This wave is more or less over. Most government entities have websites, with significant amounts of information and a degree of transactional capability.
- **Wave 2** is where most governments are today. They are enhancing the original government website/portal with more function, more complex transactions, and some more sophisticated capabilities such as shared calendars, video streaming of legislature sessions, etc.
  The parallel activity in the private sector was largely about allowing customers to access a company's core IT systems to request information about their relationship to the company, i.e., inquiring about the status of a bank account, or actually performing transactions online such as making payments or buying merchandise through an e-commerce application. Since these transactions involve sensitive data such as bank accounts or credit cards, it becomes mandatory that companies build a secure environment in which to run their e-business applications. Government needs to deal sensitively and effectively with this issue - privacy, according to some studies, is the most often quoted exposure to progress in constituent-facing e-government. However successful the initiatives are in these phases of e-

business and e-government adoption, they are the result of taking existing business processes and reconfiguring them to an electronic format. Some enterprises are taking e-business and e-government to the next level. Not satisfied with merely adjusting their business processes to align with new technologies, they are also fundamentally changing their entire organization to be completely customer-service and customer-satisfaction focused.

- So **Wave 3** is the next critical phase. It will be characterized by an increasing importance for government to become "customer-centric". Many governments are already embarking on this phase, with limited projects underway. There are significant issues associated with achieving this, however, with technology-enabled transformation being the key to achieving these new ways of interaction, rather than simply replicating online the current structures and processes of government.
- **Wave 4** lies further in the future and brings a more fundamental redefinition of the basic roles of government and the methods by which it plays them, as government questions and reforms the way it discharges responsibilities in collaboration with evolving understanding of value formed with private sector participants and other constituents.

The "e-infrastructure" which supports the move through these waves is critical. We contend that as a government moves through the waves, the complexity of its infrastructure requirement increases. Smart decisions in this area early on can ameliorate the associated difficulties. And the value of the infrastructure increases in proportion to the developing complexity.

For some governments, e-government adoption will move slowly. For others, certain phases will be omitted, enabling them to go directly to Waves 3 and 4 of the evolution. But there are three rules of thumb that will always apply:

Innovation is key to success. Innovation stems from sensing new needs and developing new responses, then implementing the necessary systems and applications to support them.

Integration increases value to constituents and efficiency and effectiveness internally. Successful e-governments will have the ability to improve the efficiency of business processes and enhance them with innovative models or technologies.

Without a flexible, scalable, reliable and secure IT **infrastructure**, integration and continuous innovation will be impossible to achieve. Ultimately, success will comes down to the quality of the e-government initiatives that enable all processes, the reliability and adaptability of the IT environment that supports them, and the vision and leadership to execute change.

The Impact of e-government on Today's IT Environment

While maintaining the traditional role of increasing organizational efficiency and effectiveness, IT departments are today increasingly required to help enable government to reach constituents in new and more valuable ways. Because IT systems are an integral part of e-government, the design and construction of a reliable e-government infrastructure is no longer solely an IT issue - it is a vital management issue generating a great deal of interest from government CIOs, senior elected officials and department or agency leaders alike.

In future, the performance - in every sense of the word - of the infrastructure will have unprecedented visibility and impact on the success of e-government initiatives. If IT fails, e-government fails, as represented by the following list of IT failure-related consequences.

- Poor return on investment: the IT infrastructure fails to meet the government business objectives.
- Dissatisfied constituents: they are unable to find information easily or execute transactions against their needs.
- Lost chances: up to 40 percent of people don't return to an Internet channel after encountering incomplete content or poor service
- Eroded image and negative publicity: through visibility of poor service, or inadvertent exposures related to privacy.

To be successful, e-governments must create an IT infrastructure that is optimized to support the new requirements. An e-government infrastructure is the set of tools that enable the execution of e-government. While the tools required to support a government process can vary from instance to instance, an e-government infrastructure is generally consistent, and comprises the following components:

- Network infrastructure
- Security infrastructure
- Application server environment
- Data and content management tools
- Application development tools
- Hardware and operating systems
- Systems management platform

These components must be complemented by operational procedures, and by people who install, launch, operate and maintain them, in order to ensure that the service levels required to operate successfully are established and maintained.

The following section describes some key design considerations for an e-government infrastructure, and provides a blueprint to help to meet the demands of e-government in the future.

Design Criteria for an e-government Infrastructure

Companies planning to deploy Internet-based e-business and e-commerce applications face the enormous task of redesigning and integrating their server, network and application infrastructures to support on-demand networked functionality – and most organizations lack the internal expertise to do so.

- Yankee Group

Successful e-government initiatives will rely on an e-government infrastructure that meets the following three criteria:

- **Flexibility** - to support rapidly evolving e-government models through the addition of new application functionality and the integration of systems and applications with constituents, partners, suppliers, and employees.
- **Scalability** - to accommodate unpredictable fluctuations in constituent demand and user workload.
- **Reliability** - to help ensure secure, continuous operation and availability of the e-government applications to end-users.

Flexibility

e-business and e-government adoption are evolving processes. Enterprises, public and private, typically start with simpler implementations, growing more complex as the business model becomes more integrated with the Internet. To remain successful in this business model evolution, it is necessary to create a flexible e-government infrastructure.

To start, the following list of infrastructure characteristics might be included:

Universal connectivity through the use of open standards. In an e-government environment, government enterprises will need to allow stakeholders - constituents (citizens and businesses), partners, suppliers, other governments and other levels of government - to have access to systems and applications through a variety of access devices and application to application interaction. It is key to use an open standards approach using Internet Standards such as Transmission Control Protocol/Internet Protocol (TCP/IP) and Secure Socket Layers (SSL) for communications, HTML/Java™-enabled thin clients, and eXtensible Markup Language (XML).

A component-based approach to application development. Rapid application development and the ability to reuse parts of existing applications will greatly accelerate the process of creating new e-government applications with the required function and linkages. Whether building or buying applications, governments should investigate application development tools that allow applications to be created from smaller building blocks (commonly referred to as “application components”), or at least tailored to the individual requirements of the e-government model.

A component based approach to infrastructure design. The e-government infrastructure will need to evolve with the changing responsibilities, priorities and activities of the government. By adhering to open standards in the selection of infrastructure elements, the elements can be treated as individual components, without jeopardizing interoperability. This approach allows governments to evolve their infrastructure gradually - adding hardware or software components, upgrading existing servers or removing elements of the infrastructure as needed.

Integration with internal and external services. Interoperability - sharing or communicating with mixed technologies across and beyond the enterprise - will be an important success factor in e-government. By integrating applications and data among constituents, suppliers, partners and employees, governments can achieve a more effective and efficient e-government model. Enabling integration is accomplished by using open standards-based infrastructure elements in conjunction with integration, which allows existing application functionality to be integrated into the new application logic.

By following a component-based approach to application development and infrastructural design, providing integration among various systems and applications, and enabling universal access to applications (with open standards as the principle that makes it all work together) governments will create a flexible infrastructure that will evolve and support their business requirements.

Scalability

One of the biggest challenges in building a reliable e-government infrastructure is predicting the demand that it will need to support. This is especially true for governments interfacing directly with their constituents and others: the number of users that simultaneously access systems, plus the workload they will create, can be very hard to predict. If an e-government initiative is successful, the customer base will grow rapidly into hundreds of thousands of users in a relatively short timeframe. Even with a static user base, such as an internal government application, and depending on when users can access the applications, demand can fluctuate tremendously during a week - or even a single day. (Please see Figure 3 below).

A scalable e-government infrastructure should be capable of handling increasing workloads while maintaining high availability and good response times - without adding significant complexity or requiring significant new resources. Scalability is important, because it helps create growth of the IT capability in proportion to need, without long periods of excess capacity.

An effective e-government infrastructure should have easily configurable components and management characteristics that remain true as the infrastructure expands. Some claim their systems are scalable, but all too often they require the other attendant processes and support staff to grow at the same rate as the technical components - which can be a costly proposition. For example, a common technical approach to increase server capacity is to run multiple Web servers in parallel. While this may be a sound initial approach to meet increased scalability requirements, it may not be as effective in handling very large increases in workload or more complex application types. With this approach, as the need for processing power continues to grow, governments could be forced to continue adding servers. This would add significant time and expense to maintain the servers and to make all applications consistent across these machines.

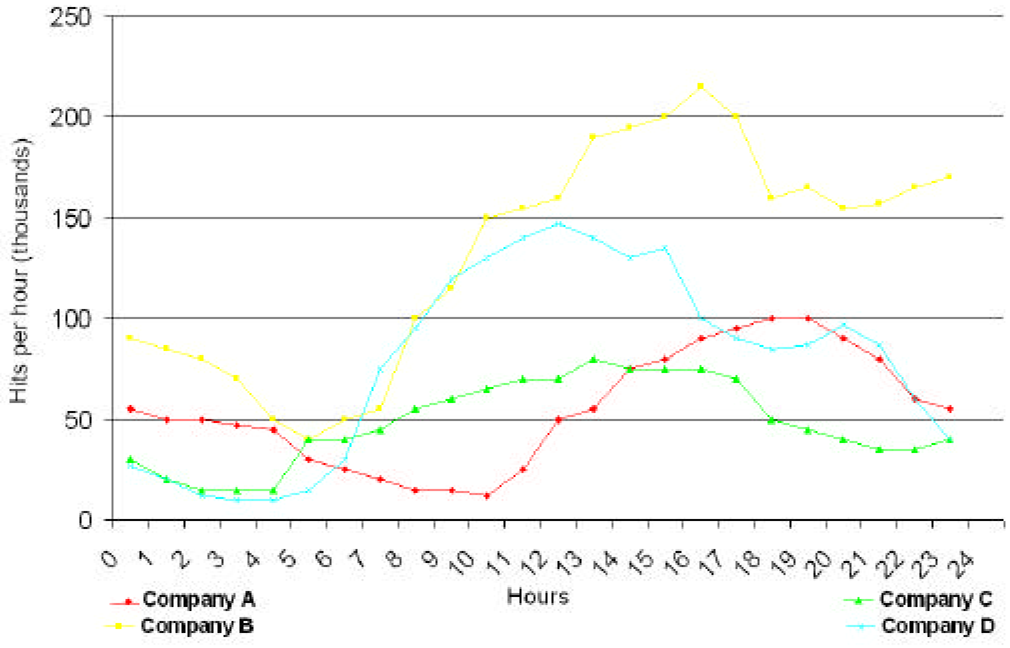


Figure 3: some typical website loads over a 24-hour period (source: "IBM Analysis of Four e-business Websites")

Alternative approaches that enhance scalability are:

- Developing applications on non-proprietary systems to accommodate added server capacity without dramatically increasing the number of servers and corresponding IT staff. Applications built around a non-proprietary architecture can be moved from one server platform to a more powerful and scalable one without the need to rewrite the applications.
- Built in load balancing, which allows governments to treat multiple servers as a single logical system, where the failure, removal or addition of a single machine does not require changes to the existing environment. These options, when considered proactively, can help avoid the need to replace components or change processes with each new advance or requirement.

Reliability

When combined, flexibility and scalability contribute to a third success criterion, reliability/availability. Reliability is the outward-facing feature of e-government - the part that constituents see, expect and depend on. When e-government infrastructures become hindered - unreliable and unavailable due to slowdowns or security breaches - the constituent experience and the rationale for undertaking the e-government initiative is threatened. It is only through adequate flexibility and scalability planning that reliability and availability can be created.

Blueprint for an e-government Infrastructure

In order for an IT environment to provide the flexibility, scalability and reliability required, governments need to develop a new kind of IT infrastructure. This infrastructure should consist of open interfaces that allow new applications and services to easily connect. It can also allow individual treatment and management of the elements within the infrastructure, including management of the overall environment. A blueprint for a successful e-government infrastructure is overviewed in Figure 3.

The blueprint consists of five logical functions:

- Web Application Servers
- Directory and Security Services
- Edge Servers
- Data and Transaction Servers
- Storage Management

Although these five functions could be implemented on either a single server or on multiple servers, separating the functions will allow for a more rapid infrastructural change - enhancing a single function without losing the interoperability of the other pieces within the infrastructure.

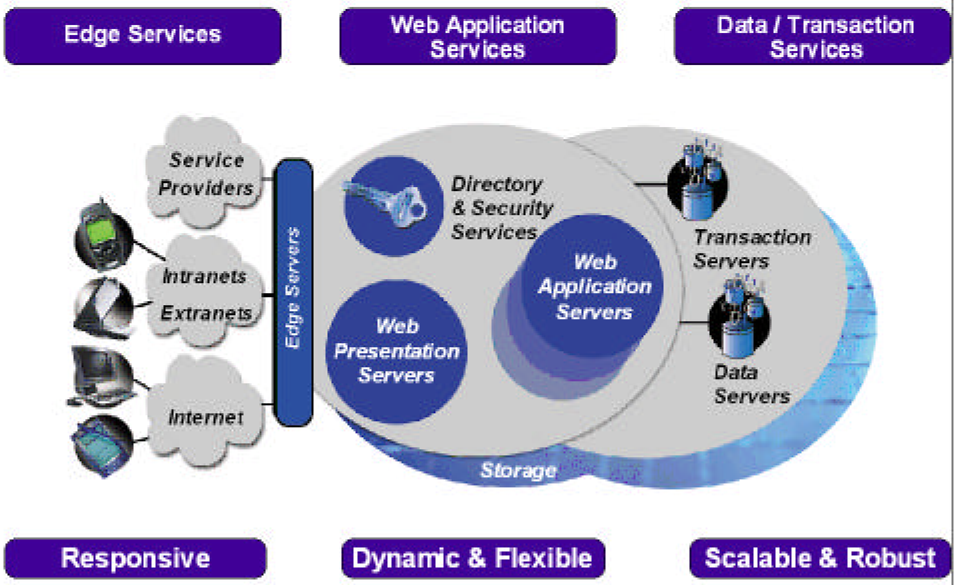


Figure 3: the blueprint for an e-government Infrastructure

Web Application Servers

At the heart of e-government infrastructures are the Web application servers. Consisting of server hardware, a server operating system and application server software, the Web application servers run the e-government application logic and manage the user interactions. While a single Web application server may be sufficient for many, others may choose to implement multiple servers - either optimized for a specific function or to provide for redundancy and scalability.

Increasingly, it is becoming important to separate the presentation logic from the application logic on these servers. The server infrastructure can do the processing work in several stages, allowing for the service of static information, or very simple transactions with lightweight dynamic data at the front end. This way, governments do not have to place load on the more complex applications that run at the back end of the system. In order to enable new e-government processes, the Web application servers should also provide comprehensive integration capability with other systems, connecting with each other and the back-end legacy systems.

Edge Servers

Edge-of-the-network servers (edge servers) have emerged as a single-function, cost-effective platform. They perform many of the computing functions that reside between the internal e-government infrastructure and the external Internet - router management, basic authentication, firewall protection, and transcoding - with the ability to support new device types and to render outbound data for the Internet in the format of the device itself.

Edge servers also improve performance in the areas of caching, load balancing and secured communications. This is important, in that transactions currently handled on a private network are moving to virtual private networking over public lines. Traditionally, technology has resided primarily on an enterprise’s own premises. The current trend is to migrate some of the functions to the network itself. Functions such as data security are likely to remain on the enterprise side of the firewall; more transient services, such as caching, are likely candidates for migration. For example, telecom operators and Internet service providers are starting to offer information caching and other services on their infrastructures, while some of the key network infrastructure providers are beginning to build this functionality into the switches that go into the network.

Security

Security requirements are also changing. Although many government websites have implemented basic password authorization, complex e-government systems will require a more sophisticated environment behind the firewall - beyond basic authorization. This is causing security functions to move from simple passwords to digital certificates, which not only provide individual user validation but also furnish different levels of validation, depending on the application or data being accessed.

The next step in security is to provide policy-based security management. A policy management server provides single and global sign-on for multiple systems, which can eliminate the need for multiple passwords.

It also manages security independently from each of the individual applications, with authorization administered and managed at a single point as an enterprise-wide common service.

Through the use of a policy-based security system, governments create a layered approach to security, offering higher degrees of protection against unauthorized access without the system becoming an unnecessary burden on constituents.

Data and Transaction Servers

Building a flexible and reliable e-government infrastructure requires seamless integration between the Web application servers and the back-end data and transaction servers. These servers handle processing-intensive and mission-critical workloads. They offer high degrees of security and application integrity, and have the ability to perform complex transactions against large volumes of data. Scalability on these servers is not achieved by adding additional server hardware; rather, by increasing the capacity of the existing system.

Storage Management

All of the four functions described above can be deployed on a single server system. The need for scalability, however, will quite often drive a need to implement an e-government infrastructure that relies on multiple systems - and possibly multiple server hardware types - to run the e-government application workload. While such an implementation can increase the scalability and reliability of the overall infrastructure, it also poses a challenge to data currency - making sure that all applications have access to the same set of data.

To meet this challenge, a government can implement a storage management solution. Storage management enables every application within the enterprise to access relevant information - independent of the type of storage the information resides on. Relevant storage mechanisms in an e-government infrastructure include:

- Direct attached storage - hard disks directly connected to a server system.
- Network Attached Storage (NAS) - hard disks grouped on a specialized storage server that is attached to the network.
- Storage Area Network (SAN) - storage capacity residing in a special storage network where administrative tasks, such as backup, are separated from the production environment. In

addition to addressing the issue of data currency, Storage Area Networks also improve the performance and administration of the overall storage environment.

Pervasive Computing

Until recently, PCs were the Internet access device of choice. Preferred substitutes, such as cellular phones and personal digital assistants (PDAs), however, are currently outselling PCs three to one. By 2003, the number of cellular phones around the world is expected to exceed 1 billion, with about 80 percent of them having some form of access to the Internet.

This rapid proliferation of new network access devices is referred to as “pervasive computing” – the migration of Web access beyond PCs to a new generation of devices that can execute any service, using both wireless and wired connections. The advantages of pervasive devices can generally be grouped in two areas: increased productivity and increased reach.

Pervasive devices with specialized, easy-to-use functions will greatly increase knowledge worker productivity. Even traditional desktops and notebooks will be used in ways that raise business issues such as manageability, security and mobility. Although the use of multiple devices per user will increase support costs, it should be an attractive return on investment by any measurement.

The key to improving user productivity is making computing simple for users by moving the complex workload away from the device and performing it on the server platform. This in turn will put more stress on the e-government infrastructure – underscoring the importance of decisions about the number and types of devices supported, the selection of appropriate tools for particular applications, and security and continuity among a variety of purpose-optimized devices.

In addition to increased productivity, pervasive devices facilitate mobility - allowing users to access applications and data from virtually any location. Mobile phones and wireless Personal Digital Assistants can already access services such as the Web, consumer and investment banking services, and online information such as entertainment offerings.

For governments, this offers a totally new way to reach constituents. By adding a wireless channel to existing applications, or building new applications that specifically exploit the capabilities of mobile devices, governments can achieve a significant increase in constituent loyalty to the e-government channel, and perhaps reach constituents who would otherwise be unlikely to participate.

As for efficiencies, few alternatives will generate the same level of compliance as pervasive computing in the field, from building or restaurant inspectors to fair hearing judges all having seamless access to historical, comprehensive case management data in real time. How much safer, more productive, and immediate might the performance of these three public duties be when the limitations of geography and land-connectivity are removed?

The improved functionality of pervasive devices will put new demands on infrastructures. Additional services necessary to fully exploit the capabilities of these devices include:

- Support for subscription services - allows users to "subscribe" to various capabilities available through "services bundles", which can be automatically downloaded and enabled on the device.
- Support for location-based services - application and device functionality that varies with the location of its user.
- Dynamically updated functionality - without user intervention, keeps software and functionality current through a transparent contact between devices and the network.
- Network and device management - manages delivery of content and services to non-PC devices - cellular phones, PDAs, Internet appliances, digital television and other new technology. This will increasingly become a key strategy in efforts to bridge the digital divide.

Technology Investment Considerations

Optimal Technology Investment

As governments continue to advance, they will likely need to continue to invest in their e-government infrastructure. More complicated service delivery models (for example, intergovernmental) and e-government applications may put higher demands on the infrastructure, resulting in additional costs for network and server hardware, software, people and infrastructure processes.

Government cannot be measured with the same yardstick as the private sector. There are significant differences in objectives, rationale for investment, stakeholders, statutory obligations, and many other factors. We do not suggest that, at least initially, governments undertake e-government solely on the basis of a cost reduction business case.

We know, however, that with a successful e-government implementation, some costs can be offset over time - online transaction costs have been shown to be significantly lower than their paper-based, face-to-face equivalents. Reductions in operational budget and personal services allocations have also been realized, allowing for the redirection of financial or human resources to other, as of yet still manual, mission critical operations.

And more effective program implementation, reaching broader constituent segments, “doing more with the same”, are all achievable objectives. At the same time it is clear that there are new revenue streams accessible to government for some services, particularly in the government to business (G2B) arena.

The objective for government should be to find its own “optimal investment curve” (please see figure 4 below), which balances infrastructure investment with the evolution of e-government initiatives.

Governments that have not found the right balance between investments in e-government infrastructure and the requirements of e-government implementation are either over-investing, and therefore wasting resources, or under-investing and running the risk of an infrastructure unable to keep up with e-government demands - which could result in poor service, sub-optimal deployment and loss of constituent satisfaction.

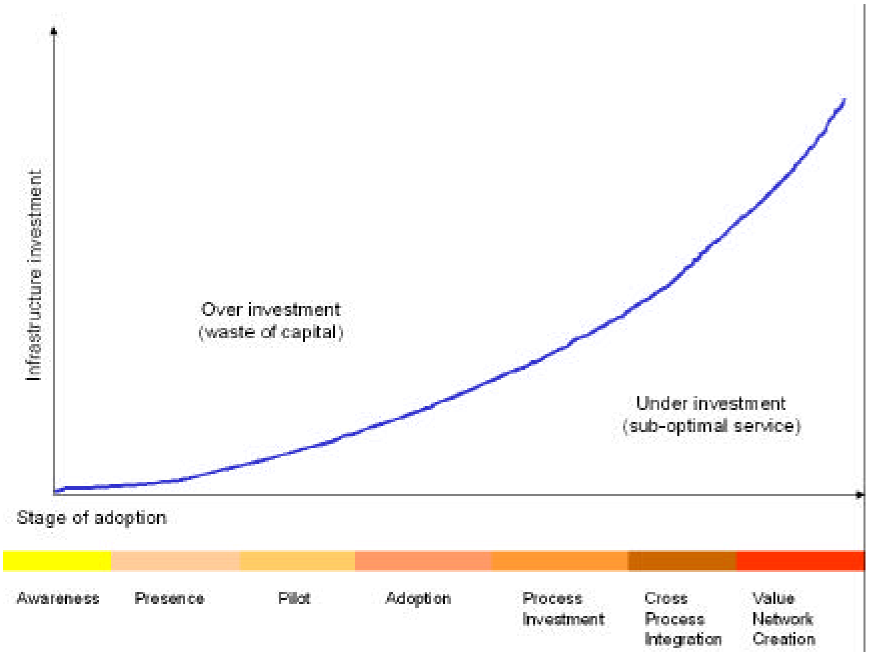


Figure 4: Optimal infrastructure investment

The Impact of Technology Choices

Another view of e-business infrastructure investing is seen in figure 5 below - the impact of technology choices. When a government is in the early phases of e-government adoption, it is logical that it would base its infrastructure on the most cost-effective technology base (say, "Technology A") for the specific business model.

As the business model becomes more complex, however, the government may need to make more investments in the e-government infrastructure to provide the required level of constituent service. At a certain point, the chosen technology may be stretched beyond its design point, resulting in either a significant increase in IT costs, or more commonly, degradation of service levels.

Had the government opted for "Technology B" in the early phases of adoption - even though it may have been more expensive to use at that point - it might have been able to sustain the evolution of its e-government objectives much further without facing a rapid increase in infrastructure cost.

As new technologies evolve and business models change, governments may be faced with switching from one technology base to another. In fact, this process may repeat itself multiple times. The optimal investment curve in this scenario will link the lowest points of each technology shown.

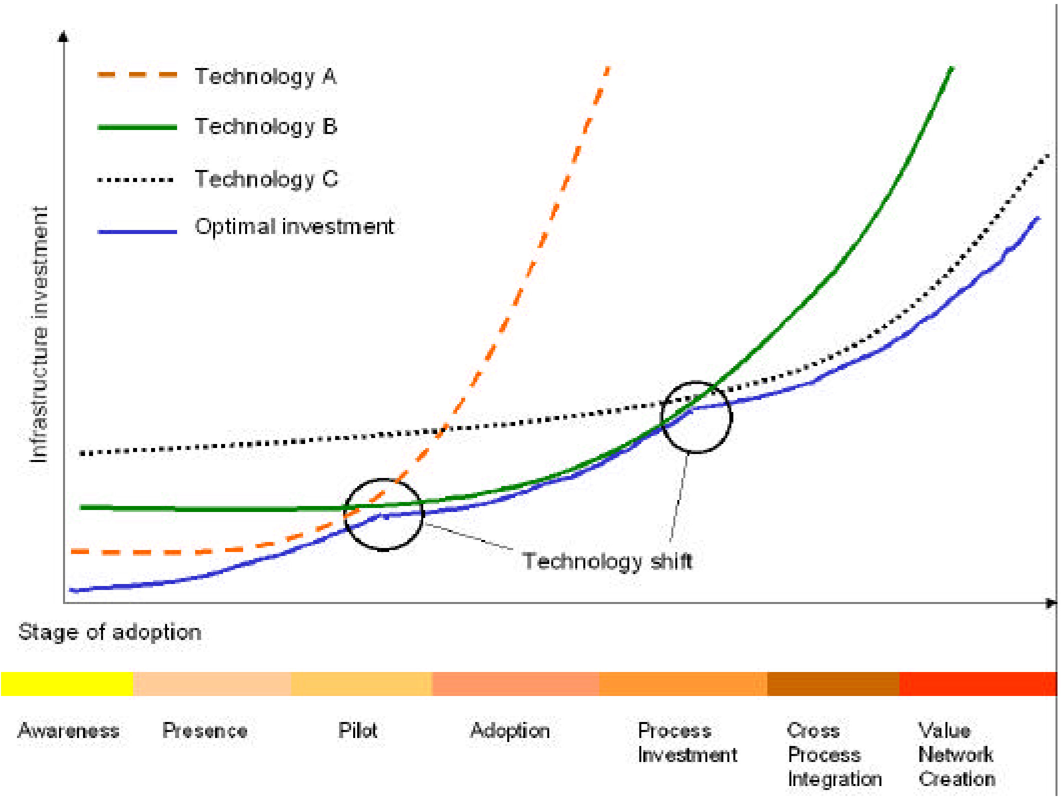


Figure 5: Impact of technology on the optimal infrastructure investment

Conclusion

> The future belongs to Web-architected applications that have best-of-breed functionality and access and aggregate resources both inside and outside the corporate firewall. Aberdeen uses the term "Internet application architecture" to describe the framework for the next generation solution.
>
> - Aberdeen Group

Managing information technology is a challenge under any set of circumstances. Creating and managing a successful e-government infrastructure requires foresight, adequate time, financial commitments, and qualified resources. Although these requirements may seem difficult to satisfy, the value of a well planned, flexible and reliable e-government infrastructure is paramount. Without it, performance degradation, security exposures and system failures will become increasingly common and damage the chances of the very initiatives that government wants to achieve. Less obvious, but equally damaging, will be an environment where the applications and IT infrastructures have insufficient flexibility to keep up with the desired pace of innovation.

For this reason, decision makers across governments will increasingly prioritize infrastructure planning and deployment in order to fully realize successful e-government. They will understand more and more that the value of an e-government infrastructure is simply the value of the e-government initiative.

At the same time, and with the many components involved in today's large e-government systems, governments are having a difficult time identifying which vendor's products best fit their requirements, and how compatible the products are with each another. Governments cannot afford to worry about integrating new technologies from multiple vendors. Clearly, government executives are not interested in becoming technology experts - they want to focus on sustaining their program delivery, executing their service responsibilities and contributing to the development of their jurisdiction. Taking all of these factors into consideration, along with the growing complexities of e-government systems, it is advantageous for governments to have a strategic relationship with a vendor that provides a complete e-government infrastructure offering, from development through deployment.

Governments, in partnership with such a vendor, should be able to build an e-government infrastructure that meets the flexibility, scalability and reliability requirements for the future, without being locked in to a single technology base that limits the incorporation of new, more cost effective technologies.

For more information

Please e-mail mark_cleverley@us.ibm.com

Please visit the IBM Institute for Electronic Government on the web at http://www.ieg.ibm.com

IBM Corporation
1133 Westchester Avenue
White Plains, NY 10604
U.S.A.

Produced in the United States of America
09-01

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.