Optimizing application
performance and
availability across
networks and systems.

# *e*Government

# Avoiding the Dotcom Disaster

"It's not the launch of *e*Government services that governments should be worried about — it's the usage of those services. Widespread usage will occur only if the public is confident of the reliability and quality of those services."

Michael Marks
Director of Service Provider Market Development
Concord Communications, Inc.
600 Nickerson Road
Marlboro, MA 01752
800.851.8725
www.concord.com

# The Rush to Deploy is No Way to Plan

In the rush to get services deployed in time to meet the aggressive deadlines published by state leaders, most government agencies overlook the absolute requirement to assure reliability and quality of those services. Governments around the world have been highly effective in leveraging private industry's expertise in e-Commerce as they deploy *e*Government services to benefit their citizens.

Governments have asked for help, and private industry has rushed in with assistance. Industry partnerships have been established to advise governments on how to use the latest technologies in their infrastructures. Consulting companies have delivered best practices advice on how to consider their citizens more like customers. More directly, CIOs from private industry have stepped in to fill government CIO positions to lead the transformation.

With the help of private industry, governments have overcome any initial sense of intimidation, and have launched aggressive plans to empower their people through IT and fundamentally change the ways that citizens, businesses, and even government agencies themselves, interact.

The one lesson from private industry that doesn't seem to get enough attention is the importance of service assurance. That lesson states simply that, when it comes to managing the reliability of an IT infrastructure, the time to worry about tomorrow is today. Although there are many reasons for the Dotcom collapse, one key factor was insufficient planning in the rush to market. Government agencies not planning now for how they will assure the reliability of their services run similar risks of failure, even as they push toward their deployment deadlines. This paper addresses how governments can plan today for successful implementation of *e*Government services as they race to leverage the power of the Internet.

The amount of mind share devoted to concerns about service reliability is far too low for government leaders to confidently assert that their services will work once a large population starts using them. Governments have announced plans and have made great progress in delivering ubiquitous, anytime, anywhere access to seamless government services.

Encouraged by the concept of citizens as customers, governments have deployed customer-centric services designed around citizens' lifecycle needs, as opposed to designed around the agency structure of government. There seems to be no limit to the types of services that governments can provide, on a 7x24 basis, acting as a "one stop shop" for serving their citizens.

Those government leaders responsible for the launch of these new services should ask themselves these questions: Have they swung too far in how they look at technology deployments? Have they become entranced by the equivalent of the private sector's dreams of market share dominance—universal access by the whole population to a one-stop shop of a myriad of life-enhancing government services, available anytime, anywhere; focused for now on time to market, and content to worry tomorrow about managing the complexity of the network and the range of services being considered?

It's too comfortably easy to draw a cloud around the multitude of access devices that citizens will use to obtain services and simply label it "network", with little or no regard to the complexities involved in managing a heterogeneous network comprised of emerging and traditional technologies. It's easy to underestimate the management implications when formerly isolated agencies, each standardized on separate technologies, vendors, and operational processes, are forced to integrate in an automated way. It's too easy to make assumptions about how capacity will be added as services are brought to new geographic areas, and as the population increases their usage, rather than ensure the proper capabilities are in place to time capital expenditures to stay abreast with demand.

# *e*Failure Is Not An Option

It's difficult enough for governments to tackle the deployment challenges, technical and political, involved in offering new services via the IT infrastructure. Why must they also tackle the management challenges at the same time? The reason is that, for *e*Government services, the stakes are higher than they were for private industry during the Dotcom era.

***...for eGovernment services, the stakes are higher than they were for private industry during the Dotcom era.***

For private industry, the Dotcom collapse was cushioned by the presence of the reliable "brick and mortar" companies. Alternatives to on-line services existed. Customers could buy their groceries in the good, old-fashioned supermarket, if they weren't satisfied with their on-line delivery. Smart businesses hedged their bets—sure, they offered on-line services, but they did so in addition to their traditional products and services, just in case the on-line experiment didn't work out.

In many cases, governments don't have the luxury of failure. The opportunity to instantly and effectively bring critical health information to remote populations simply doesn't exist without the IT infrastructure. When a centralized government shuts down for business at the end of the day, there simply are no services to be had, without the IT infrastructure. If a citizen needs a form to obtain permission to open up a new business or to obtain benefits, he or she must simply queue up in the morning. The ability to ensure public safety requires a modern IT infrastructure. The old way of doing business—separate, disparate systems with no communication between them - is no longer sufficient. Reliance on IT is a must, and given that reality, governments must recognize the need for up front planning on how they will assure quality and efficiency of services.

***In many cases, governments don't have the luxury of failure.***

The time to peer into that network cloud and assess the management implications is while the service is being deployed, not afterward. Today, not tomorrow. Whether you decide to outsource the management of your IT infrastructure or manage it yourself, you need to ask the critical questions today about how to assure the reliability and quality of your *e*Government services in an efficient and effective manner.

# End User Adoption Pitfalls

Today's governments haven taken a great first step in recognizing the need to focus on "citizen-centric services," that is, services that are provided based on an understanding of the lifecycle needs of citizens, rather than merely representing the existing government agency structure on-line, and expecting citizens to navigate a new "e-Bureaucracy."

Taking another lesson from the business world, governments have segmented the market, and provided services organized by customer need, such as "education," "marriage and adoption," "employment," and "retirement and health care," etc. Governments have recognized the positive impact to customer satisfaction that results when they hide the confusing multitude of agencies with which a citizen must interact in order to plan for these lifecycle functions.

But the implications of the next step in customer segmentation haven't yet been addressed. The next way to segment a market for technology products and services is by the degree to which certain populations are receptive to the idea of using new technologies. The different populations illustrated in Geoffrey Moore's Technology Adoption Life Cycle[1] respond to technology in fundamentally different ways, and the importance of service quality becomes more and more important as services are rolled out to broader sections of the population. The initial sets of customers, the innovators, and the early adopters, appreciate technology for its own sake, or for the potential of technology to make huge, fundamental improvements in the existing way of life. From a service assurance perspective, these people are easy to please—ease of use and reliability are not important—the simple existence of the technology and its future impact are the critical factors. These technically savvy groups comprise only a minority of the population, generally less than 20%.

The majority of the population is not overly enamored of technology. Often comfortable with the status quo, they must be convinced of a significant improvement in their daily lives by using technology in new ways. There is little tolerance for services that are difficult to use, erratic in their availability, or sluggish. The majority of potential users have quality and reliability uppermost in their minds.

Simply stated, without up front consideration of assuring reliability and quality, deployment of *e*Government services will fail to benefit the vast majority of the population. Without taking these steps, the successful deployment of new services won't matter. Governments need to do the kind of planning that private industry failed to do in the era of Dotcom hype—focus on managing service and reliability so end users "make friends" with technology quickly when their initial experience is a positive one.

***Simply stated, without up front consideration of assuring reliability and quality, deployment of eGovernment services will fail to benefit the vast majority of the population..***

[1]"Crossing the Chasm," Geoffrey A. Moore, HarperBusiness, 1999

# Ensuring a Positive First Experience

A true *e*Government is one that is always available. A government that promotes a 7x24 *e*Government service needs to make sure that that service truly is available 7x24. Continuous monitoring, early detection of potential problem indicators, rapid diagnosis, and fast recovery from problems comprise the minimum effort that must be devoted to service assurance. Providing this level of service doesn't need to mean armies of highly trained network operations staff. Management software can automate the critical service assurance functions to provide this level of reliability, easily, quickly, and with high quality. Management software deployed on the servers which provide information to the public, can continuously monitor the critical server processes and resources for signs of impending trouble, provide early notification to operations staff of problems, and can often be instructed to automatically take the requisite actions to recover from commonly expected problems, all without manual intervention.

Although constant availability is the primary service assurance requirement, rapid response time is a very close second. The problem is that slow service is almost as bad as no service. It does no good if a service is available but is so sluggish that it takes an unacceptable length of time to get information from that service. Governments, not especially known for their streamlined "brick and mortar" services, have the opportunity to use management software to fundamentally change citizens' experiences in dealing with the electronic versions of their services. Management software can assure the fast response of a service by automatically conducting periodic active tests of response time. Periodic tests that track the latency at the network level, and at higher protocol levels, can identify when citizens experience delay in their routine *e*Government interactions, such as sending e-mail, retrieving information, and processing transactions. Early identification of sluggishness is one thing, but identifying and correcting the source of the delay is the key problem. Management software with the ability to monitor all of the infrastructure involved in delivering services, from the network transport technologies, to the servers on which the service content is housed, and to the actual content itself, can automate the identification of bottlenecks, so prompt action can be taken to resolve the problem.

***Governments, not especially known for their streamlined "brick and mortar" services, have the opportunity to use management software to fundamentally change citizens' experiences in dealing with the electronic versions of their services.***

# Harnessing the Moving Target of Peak Usage

The problem of assuring the quality of *e*Government services is more complicated than it first appears, because it is a moving target. Response time of any service is driven by usage patterns, which vary, according to time of day, day of the week, even season. For example, an employee using the Internet should expect slower response time during lunchtime than at other times of day, due to the fact that other workers just like her are likely accessing the same infrastructure. A government which offers citizens the ability to file taxes on-line should expect that the infrastructure supporting that capability will be busier around the season of tax filing deadlines.

To maintain efficiency as well as quality, operations staffs supporting *e*Government services must account for these normal, expected, time-based variation in services before they determine whether or not a problem exists. The question is not whether the service experienced is slow, but whether or not the service experienced is different from what is expected, for that period of time. Management software with the ability to analyze the trends in historical performance, project future expected behavior based on those trends, and send alerts when the performance deviates from normal, expected behavior, is the key to such efficiency.

Scale is the other dimension that is constantly changing, as the population of citizens using *e*Government services increases. Confidence in the reliability of services causes an increase in the proportion of citizens who use *e*Government services in those areas in which they are already available. Usage increases across wider geographic areas as services are launched in more remote areas. As the usage load on the IT infrastructure increases, the limits of what constitutes acceptable performance are approached. Governments must wrestle with the resulting capacity planning problem—at what point of service usage are additional capital expenditures required in order to ensure reliable and high quality service for all users?

Governments have typically addressed the need to deal with expanding growth by grossly over-provisioning. Rather than be caught short with insufficient resources, governments prefer to be safe by purchasing far more bandwidth, more networking equipment, more servers, more application licenses than they actually need. While this strategy does lead to a level of comfort, it also unnecessarily adds costs and increases the likelihood that governments will be stuck with obsolete technology as new innovations are developed. Management software with predictive capabilities, the ability to project future capacity needs based on past usage trends, allows governments to make intelligent capacity planning decisions. The capability to project exactly when and where additional capacity must be ordered, such that it is installed and operational in time before predefined usage limits are reached, allows governments to spend money neither too soon nor too late to support an ever-growing usage base.

It's not the launch of *e*Government services that governments should be most worried about – it's the usage of those services. Keeping in mind the concerns of the majority of potential users – governments must take active steps to ensure that citizens will have confidence in the reliability and quality of *e*Government

***It's not the launch of eGovernment services that governments should be most worried about – its the usage of those services.***

# Harnessing the Moving Target of Peak Usage (continued)

***Widespread usage of eGovernment services will occur only if the majority is confident of the reliability and quality of those services.***

services. Too many users have a low level of tolerance for poor performance. When they finally take the big step to try an on-line service, they will never come back if the service is not there, or too slow the first time. "I tried that once, and it didn't work. I was better off standing in the queue, then waiting for my screen to refresh." Widespread usage of *e*Government services will occur only if the majority is confident of the reliability and quality of those services. Without taking the required steps, all of the social gains promised by the Internet are at risk.

# The Irony of Simple *e*Government

Historical agency autonomy, combined with the complexity of the IT infrastructure needed to support a real *e*Government initiative has created quite a paradox. Simple, easy to use *e*Government services means complex management headaches for IT professionals.

Governments typically discuss their planned service deployments in the context of at least three tiers, increasing in both benefit to their citizens and complexity of IT infrastructure. The highest value services also present the most complicated service assurance problems. The first tier is a simple one-way delivery of government information through an on-line presence. The next tier improves citizens' interaction with government, by allowing citizens to engage in two-way interaction with individual government agencies to do simple things like express their views on a proposed policy, or download a publication or permit. The more complex interaction that comprise truly transformational services make up the next tier. These interactions are multi-step transactions, which can cut across a variety of agencies. Most governments acknowledge that the main challenge to achieving this last tier is not so much technical, as it is cultural and organizational. In order to provide efficient, easy-to-use services to its citizens, government agencies that have been historically independent will need to coordinate with one another to unprecedented degrees. But once these organizational challenges are overcome, the complexities involved in assuring the reliability of these multiple tiered transactions become readily apparent.

As private industry has learned through its eCommerce experiences, the service assurance challenges increase along with the complexity of the IT infrastructure supporting each tier. The infrastructure to support two-way communication between government and citizens increases beyond that required to allow citizens to passively view agency information from an on-line presence. In addition to web servers—messaging, directory, and network services are also required to enable communications with citizens to process simple interactions. In order to support more complex transactions, governments build infrastructure that supports multi-tier processing of applications. These infrastructures often combine a front-end web server, with servers running various applications, and other back-end servers running large databases. Security and authentication services are required to ensure the safety of citizen information. Facilities to provide redundancy and back-up services are often also deployed, further complicating the infrastructure. Ironically, the evolution of *e*Government to provide easy-to-use services to its citizens creates a hugely complex service assurance problem for the operations teams whose job it is to manage these infrastructures.

> ***Ironically, the evolution of eGovernment to provide easy-to-use services to its citizens creates a hugely complex service assurance problem for the operations teams whose job it is to manage these infrastructures.***

# The Seamless User Experience

Without management software, governments have no means of efficiently assuring the reliability of the various technologies and components underlying the IT infrastructure. Management software contains the intelligence to understand the key performance indicators for all types of technologies, no matter whether that technology is a network transport device, a server housing a critical application, or the application or database itself. The most effective management software tools use a consistent, uniform way to present the critical information on how well these components of the IT infrastructure are performing, so that the operations staff charged with managing these components don't have to have the expertise to understand the deep technical nuances of each vendor's particular piece of software or hardware. This consistent capability becomes especially effective as the IT infrastructures of previously independent agencies are joined together to create seamless services.

In a majority of cases, it is likely that the technology and vendor equipment that one agency has traditionally standardized on is different from that of the other agencies with which they are now forced to integrate. Reducing the technical requirements for supporting a service allows services to be supported more quickly and efficiently, a particularly useful capability in an era of shortages of qualified IT staff.

In addition, top management software packages allow operations staff to use the same workflow to manage network technologies as they do for systems, applications, and databases, thus reducing the number of disparate service assurance tools required to support the service. Reducing the number of tools to learn, and management software vendors with which to interact, also improves the economics and efficiency of a government service.

# Easier, Faster, Better – The Recipe For Early Adoption

The motivation to consider the service assurance requirements and the management software capabilities today, rather than tomorrow, is clear. If technology is the enabler by which governments empower their citizens and create positive investment climates for their businesses, then management software is the means by which quality and efficiency are assured. Although the challenges of managing today's complex, heterogeneous IT infrastructures seem daunting, leading management software solutions have the capabilities that governments need to ensure that their services are supported effectively when they are launched.

With today's leading management software products, governments have no reason to put off consideration of how they will ensure the reliability and quality of their *e*Government services. Deploying and operating a best-of-breed management software solution doesn't have to involve months of expensive design consultants, architects, and trainers. Management software that provides the critical capabilities necessary to manage the largest of today's IT infrastructures has been installed, tuned, and operational in weeks not months. Management software contains the intelligence required to understand the key performance metrics of the variety of technologies comprising the IT infrastructure delivering today's *e*Government services. Armed with this knowledge, governments can efficiently staff their operations teams to support the most complex infrastructures, with a minimum of training, time, and effort.

> ***If technology is the enabler by which governments empower their citizens and create positive investment climates for their businesses, then management software is the means by which quality and efficiency are assured.***

To ensure quality, management software with built-in intelligent algorithms can identify not just when a problem is occurring, but also when a service degradation is about to occur in the future, so that action can be taken to identify and fix the problem before service to citizens and businesses is impacted. Management software with these advanced capabilities is available today, and in use by governments around the world. Comprehensive, integrated, uniform support of networks, systems, and applications is available from companies like Concord Communications. The time to consider using this type of software to assure reliability and quality is now.

concord.com

**Concord Communications, Inc.**
Worldwide Headquarters
600 Nickerson Road
Marlboro, Massachusetts 01752
800-851-8725
P 508-460-4646
F 508-481-9772

Latin America
- Mexico +52 5322 3241

**Concord Communications Europe**
Regus Teleport Towers
Kingsfordweg 151
1043 GR Amsterdam
The Netherlands
P +31 (0) 20 491 9610
F +31 (0) 20 491 7350

- UK +44 (0) 1784 898 298
- Central Europe +49 (0) 8106 30510
- Southern Europe +33 (0) 1 4692 2420

**Concord Communications Asia Pacific**
Level 4,
107 Mount Street
North Sydney NSW 2060
Australia
P +61-2-9965-0600
F +61-2-9929-0411

- Japan +81 3 5778 7629
- Singapore +65 333 1377
- Hong Kong (852) 282 48978