



How to take the fear out of bringing government systems online

Introduction

Government agencies often receive demands for online services, both from constituents and from other governmental entities. Such agencies may be interested in providing self-directed customer service, Web-based transactions, online information resources and streamlined communication channels. Adding to the pressure, the Government Paperwork Elimination Act (GPEA) mandated that by October 2003, transactions with the federal government had to be available online unless there was a compelling reason to maintain a primarily paper-based system.

Online systems can help:

- *Deliver services directly to constituents at lower cost with greater flexibility than traditional delivery mechanisms*
- *Reduce operational expenses, especially with limited staff and budgets*
- *Deliver a tangible return on investment*
- *Improve operational efficiencies*
- *Streamline the flow of information between governmental entities, as well as between agencies, businesses and taxpayers*

This last point is particularly crucial. Many terrorist actions highlight the liabilities of unlinked government information systems and emphasize the need for better coordination. Previously isolated databases should now be communicating with one another to help promote the success of homeland security and similar initiatives that cut across traditional local, state and federal boundaries.

Why hesitate?

Despite the compelling reasons to make transaction, commerce, information and communications processes available online, government organizations have been significantly slower than much of the private sector in adopting Internet and other networking resources. There are several reasons for the delay, including:

- ***Fear of losing the public trust.*** *Government agencies understand the importance and sensitivity of the information they collect. If any income, social security numbers or other key personal information were to become public, the repercussions in terms of loss of goodwill and potential criminal liability could be severe. Government databases also carry tremendous amounts of information that might be of great value in the wrong hands – everything from personal identification resources to classified documents and archives. If data is lost or stolen, the public's trust in the government's ability to safeguard sensitive information could be compromised or even destroyed.*
- ***Anxiety over national security.*** *Concerns about online attack and misuse, including espionage, have made it clear that a concerted attack on Internet-based technologies can create a sense of panic. On a pragmatic level, many governmental entities feel that it is better to err on the side of caution. In other words, no information access is better than access that places anything at risk. Even though the private sector and the military have long track records of successful information security practices, risk adverse managers may use security as an excuse to avoid innovation.*
- ***Concern over potential internal abuse.*** *While many government employees at a variety of different levels have access to sensitive information, bringing that information online presents new opportunities for misuse. Imagine the havoc that a disgruntled government employee could wreak on an organization by quietly deleting critical information or publishing sensitive data on a Web site. Without a full understanding of how to supervise and enforce access to online information, agency managers may be wary of introducing additional levels of technology and transparency into their daily operations.*

- ***Inadequate in-house skills and knowledge.*** *Government agencies frequently recognize the basic need for secure, online information services. In contrast, they often lack employees who understand the technological intricacies of online information protection. Therefore, they may latch onto products that sound like they will protect information systems, without making sure that they will actually achieve what they promise. Alternatively, they may begin a deployment, only to back off once the scope of the commitment is fully understood. The relative scarcity of security expertise and high salaries this staff commands only complicates the equation.*
- ***Limited budgets and staff resources.*** *Protection of online resources is not a core competency for many governmental entities. As a result, it can be difficult for agencies to establish a clear, tangible benefit for information protection expenditures. With inadequate funding and already overburdened staff, good security practices can be difficult to establish and enforce.*

While each concern is valid, the reasons for not speeding the development of secure online information systems may soon be irrelevant. Directives set in Washington are forcing information protection compliance on even smaller governments and agencies. Standards such as the Federal Information Security Management Act (FISMA), ISO 27002 (a ten-part, widely recognized security process standard) and legislation like the Gramm-Leach-Bailey Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) have focused attention on the flow of information through and across departmental lines, and out to the general population.

The basics of government-based online information security

Fortunately, federal, state and local governments have established models to use as they build appropriate online information security strategies. Many agencies already deliver key services online, including license renewals, check distribution, payroll processing and much more. These operations already operate securely, with careful attention to people, processes and technology that:

- **Promote system availability.** *Systems must be up when needed. If they are not, people may stop trying to use them. More importantly, people may associate “not there when I need it” with the agency in general.*
- **Help confirm data integrity.** *Constituents should feel secure that no one can tamper with their online transactions and that databases are accurate and reliable. Generally, people do not want to find out that they are on the FBI’s “most wanted” list as part of a prank or to discover that nuclear munitions listed as secured are, in fact, missing. In other words, data that is not reliable is often much worse than no data at all.*
- **Increase data privacy.** *If constituents believe that private data might be openly available to others, they may avoid using any systems that might make their information openly available. Since human nature tends to distrust technology when it comes to privacy, even the slightest appearance of a lapse may be enough to deter widespread acceptance of any online initiative.*

In addition to the basic needs detailed above, information sharing programs that address national security and other cross-jurisdictional concerns should also:

- ***Help anticipate system attacks/misuse*** by obtaining current online attack trend information from reliable sources. Any trusted relationship is only as strong as its weakest link. Agencies should be sure that their partners properly anticipate and respond to threats.
- ***Promote secure information sharing*** with security providers and law enforcement agencies. Failure to share information and coordinate response can hamper the global threat recognition necessary to deter coordinated attacks. However, this information itself should be carefully protected from attack and misuse as it moves across multiple jurisdictional boundaries.
- ***Increase protection of shared security information resources***, including both public and private threat recognition and response centers, security information databases and research facilities. Since ownership of many of these resources is shared jointly among multiple participants, secure operations should be established from the outset, with clearly delineated responsibilities for all participants.

How to create a more secure information protection platform

There are two basic components in an effective information security strategy: technology and expertise. These elements apply equally to in-house or managed security solutions.

A pervasive protection platform provides wide-ranging, flexible and adaptive protection across networks, servers and desktops. In other words, it is designed to continuously assess vulnerabilities and help identify active threats, no matter where an online risk exposure appears. The platform should encompass a wide range of security technologies – active blocking, malicious code control (active content and/or antivirus), public key infrastructure, virtual private network vulnerability assessment, policy distribution and enforcement, intrusion prevention, application protection and security decision support – in an easy-to-use, centrally managed framework. As a result, protection platforms address specific organizational needs and operational IT functions.

The IBM® protection platform includes all of the above-mentioned components. It provides preemptive protection across networks, servers and desktops, and applications.

The platform can be deployed in a simple configuration to begin with, then more comprehensively if a return on investment is realized. Centralized configuration and management mean security operations – including incident management, policy distribution and reporting – can be better integrated throughout the organization. Automated policy distribution and audit capabilities carry the bulk of day-to-day security operations, so the government agency can focus on the actual services and transactions it delivers. This can reduce the time and expense of security management, potentially freeing up more resources for other tasks.

IBM Internet Security Systems expertise: research, analysis, education and improvement

Technology is only half the information security battle. Vulnerabilities, threats and response procedures evolve rapidly and continually. Therefore, the foundation of an effective protection platform should include security intelligence, experience and expertise. Without proactive research into new threats and attack trend analysis, ongoing education and proper security procedures, security solutions may be unnecessarily obtrusive towards normal operations and increasingly ineffective over time.

The IBM Internet Security Systems (ISS) X-Force® research and development team conducts primary security research into threats and vulnerabilities which is infused into all IBM ISS products and services. Clients benefit from the most up-to-date security intelligence from around the world, designed to keep them protected ahead of Internet threats. The X-Force also shares security information with public sector entities in order to protect critical infrastructure from online threats.

Managed security solutions can relieve IT staff and enhance protection

For many government organizations, outsourcing security management to a trusted expert relieves the burden on IT staff and enhances overall protection. With a managed security solution, the agency works with an established security partner with government experience.

Managed security services provide a single point of contact for a variety of security needs. Since security hardware, software and staff are managed by the solution vendor, agencies are positioned to save on staffing and equipment expenses. Operational security expenses become more predictable fixed costs and may be easier to approve, especially if the security provider is already an authorized vendor of other services.

Best of all, managed security solutions place the bulk of security responsibility on the service provider. Since managed security service providers concentrate solely on security, they have the potential to see a wider variety of threats, most likely have a deep investment in staying abreast of breaking trends and often have emergency response capabilities.

As with all technology purchases, those in charge of establishing and securing government systems should aggressively research the company's track record with respect to security. Check the company's references. Review case studies thoroughly. Look for best-of-breed technology, experienced consultants and an established methodology for addressing today's – and tomorrow's – government IT security needs.

Conclusion: proper security practices can position agencies to thrive online

The demand to bring government services and transactional applications online is growing daily – even if concerns are slowing some forward progress. Fortunately, there are successful, proven models for how to move government services online securely. Whether in-house or through a managed security solution, the process does not need to break the bank or disrupt normal operations. The key is selecting the right information security partner that can help ensure the availability, integrity and privacy of government information and systems. As government agencies continue to deliver online services to their constituencies, integrated, well-designed protection platforms will help agencies make the transition smoothly and securely.

About IBM Internet Security Systems

IBM Internet Security Systems (ISS) is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM Internet Security Systems X-Force® research and development team – a world authority in vulnerability and threat research. For more information, visit www.ibm.com/services/us/iss or call 1 800 776-2362.



© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
09-07
All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Internet Security Systems and X-Force are trademarks or registered trademarks of IBM Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

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