

Your Privacy, Security and Assets Are Just a Few Double-Clicks Away

By RALPH CAMPBELL JR.
State Auditor of North Carolina

It is difficult not to be stunned by the explosion of information technology which has occurred in just the last few years. There are now more than 100 million Internet hosts on the World Wide Web. Five years ago, there were just over 6 million.

Over 49 million personal computers were shipped in 2000, and nearly two-thirds of American homes are now connected to the Internet. E-commerce is no longer some fanciful futuristic dream, but an economic reality that generates billions of dollars in sales.

For government, the Information Age has opened up boundless possibilities for improving access to public records, for conducting business with citizens and for tearing down the bureaucratic walls and "turf protection" that has hindered interagency cooperation for decades.

As government services have cautiously crept out onto the Internet, our citizens have shown that they would far rather be on-line, than standing in line. Without question, technology has the potential to dramatically change state organizations and operating practices, create new opportunities, reduce costs, generate economic growth in areas previously left behind and, most importantly, improve the delivery of services to our citizens.

But the limitless possibilities of the virtual world have a dark side: almost limitless exposure to risk.

Government's ever-expanding reliance on computer systems, applications and networks that tie agencies together, both internally and externally, are growing increasingly complex and expensive. That complexity exposes agencies to a risk of invasion that grows with each new advance in technology.

Cyber-attacks, system failures and natural disasters pose a greater risk now than ever before to shutting down the operations of government, with results that can be disastrous.

The risks can be as simple as a technologically skilled citizen who hacks into government records and erases a traffic conviction from his record. Or they can be as complex as a computer-skilled criminal with a wide range of digital tools who breaks into a government bank or investment account and transfers funds electronically through several states or countries to an off-shore numbered account.

A bored high school student, left at home alone because of bad weather or a latchkey kid with two working parents, could spend his time defacing a government website with graffiti. Or an enemy power could subtly alter information on a news or military site to spread panic or affect the timing of an operation.

The September 11 attacks on the World Trade Towers and the Pentagon showed us how vulnerable we could be to coordinated, physical attacks by terrorists.

Unfortunately, we may be even more susceptible to such attacks in the cyber-world.

Coordinated computer attacks have the potential to disrupt the technology infrastructure used by our banking and financial institutions, telephone systems, the national power grid, water resources, and oil and gas distribution networks. The failure of any of those systems could be devastating.

While state governments have scrambled to implement new technology and its potential for improving services, they have been slower in recognizing the accompanying risks. But those risks must be managed, just as technology growth must be managed to be effective.

An effective statewide management strategy for information technology involves key leaders, who establish IT policies and procedures; professional technical staff who operate in accordance with those policies and procedures; and auditors who regularly check technology operations against those policies and procedures and generally accepted standards.

All three groups must recognize security as an underlying principle for technology development.

In the early years of technology development, agencies acted on their own to purchase information systems that seemed to address their individual needs. There was no oversight, no standards and no policies in place to make sure that the systems did what was needed.

The result was a hodge-podge of computer systems using different programming languages; systems that could not talk to each other; and disjointed systems that duplicated the same operations performed elsewhere in government. It was digital chaos, presenting so many problems that security rarely was even a consideration.

We know better now what must be done. Technology development must be coordinated through a governance system that brings every stakeholder to the table: elected officials, agency leaders, technicians, information system auditors, vendors and knowledgeable members of the public.

This governance structure can set up a standardized architecture and policies that assure compatibility and best practices. And it also can ensure that security is a key part of the development plan, not just an afterthought.

Audit organizations, while they must maintain their independence, should be key strategic advisers as those technology plans are put together and systems deployed. Not only will their input help ensure that security issues are addressed early, it also will ensure that auditors who must later check the systems are fully aware of their intended use and functions.

Beyond that, computer security awareness must be woven into the cultural fabric of government at every level. Every computer user should feel a duty to use effective passwords, to guard system accessibility and to report risks and incidents they observe. Security is everyone's responsibility.

Information system auditing is a well-defined profession that is governed by established standards, guidelines and procedures published by an international standards board.

Like virtually every other business in these times, accounting and auditing have undergone a revolution in how they perform their work. Auditors have traded green eyeshades and arm garters for laptop computers and scanners.

Financial records, once relegated to ledger books and journals, are now more likely to be electronically calculated, stored and distributed. Information system auditors, among other things, make sure that the computer programs used to keep those financial records are operating properly and do not contain hidden "bugs" that could lead, either consciously or unknowingly, to fraud.

Information system auditors are able to assess an agency's technology planning and organization, implementation, support and monitoring. They are fluent in the wide range of computer operating systems, networks, security software and financial applications.

This specialized branch of auditing is helping to assure the reliability of financial statements. As technology has raced through government operations, auditors generally have been limited to checking what data was entered into the computer and what data came out. Information system auditors are helping to audit through the computer, not around it. A new standard for the profession requires auditing through the system so that Information system auditors can assure themselves of the security and reliability of an application. With most government financial records now stored on computers, information system auditors are an integral part of virtually every audit.

Information system auditors also play a critical role in assessing new technology developments, identifying the critical systems that must be protected if government is to function and ensuring that all agencies have recovery plans that will help them get back in business after a cyber-attack, natural disaster or other interruption.

In the wake of September 11, security measures which at one time might have seemed excessive should now be considered a minimum effort. The war on terrorism requires a different sort of vigilance because of the threat not only to physical resources, but to virtual ones as well.

Government organizations, I believe, should establish methods for documenting information technology system failures, and quantifying the cost to taxpayers. Every time a system goes down, whether from intentional causes or unintended "glitches," there are costs associated with it. Verifying those costs would show both users and taxpayers the impact of information systems on our work and the necessity for an increased awareness of security.

The Institute for Security Technology Studies at Dartmouth College recommends a number of “best practices” for computer security. Those include:

- Regular updates of operating systems and software;
- Enforcing strong password policies;
- Locking down systems to limit physical access;
- Disabling all unnecessary services;
- Installing and updating anti-virus software; and
- Employing intrusion detection systems and firewalls to protect data.

These basic security procedures apply to virtually any computer system or database used by government. Critical systems will need even tougher security measures to keep them secure.

But be aware that even the most complex security arrangements are likely to be undone by a committed hacker using the electronic tools that are now widely available to the public. Vulnerability tests conducted by states and the federal government have shown over and over again that even the most secure IT systems can be compromised, often in an embarrassingly short time.

The General Accounting Office and State Auditors across the country have been working together in the Joint Information Security Audit Initiative. This effort, involving federal agencies, state auditors in North Carolina; Kentucky; New York; and Texas; as well as local government auditors from Orange County, CA; and Tallahassee, FL, has produced a guide for strategic planning in Information Systems Security Audits.

The guide helps audit organizations of any size in establishing or enhancing its capability for auditing information systems. One of the key techniques for that auditing is vulnerability testing, which shows just how secure government computer systems are.

A word of caution, however. Vulnerability testing is a complicated field that requires both specialized tools and specialized knowledge. While the testing is considered a normal part of information system audit practices, it is helpful to have the support of lawmakers and other agencies in conducting such tests. And it is critical that the results of those vulnerability tests be declared exempt from public record statutes. Otherwise, the state will simply be handing crucial information about its computer networks to cyber-invaders.

Secure back-up systems, regularly used, and off-site storage of electronic data is absolutely essential to keep government systems operating when an attack or disaster strikes.

As we learned from the World Trade Centers attack, off-site storage needs to be far off-site. Federal agencies housed in a building beside the twin towers were forced to flee after the attack. And when the towers collapsed, their building was left in shambles.

Unfortunately, the “off-site” storage center used by several of the agencies was on another floor of the same building, so in one stroke they lost both their original electronic records and their back-up copies. Their records had to be reconstructed, where they could be, by hand.

As the technology revolution has overwhelmed us, many public officials have shied away from the fray, reluctant to get involved in a technical area in which they were not proficient. The days when that luxury was possible have long since disappeared.

To lead in the Information Age, you must take an active role in establishing information technology strategies, implementing specific projects and helping to formulate public policies that recognize both the historic openness of American government and the need to protect critical data.

The Harvard Policy Group on Network-Enabled Services and Government has developed eight “imperatives” for leaders in the Information Age. They include:

- **Focus on how Information Technology can reshape work and public sector strategies.**
Do not make the mistake of delegating all responsibility for technology to technicians. Look for opportunities to improve services and build support for such initiatives.
- **Use IT for strategic innovation, not simply tactical automation.**
Think outside the box! Think about fundamentally re-designing organizations and practices, rather than just using automation to entrench old paper-based operations.
- **Utilize best practices in implementing IT initiatives.**
Do not approach as primarily a technology problem. Technology implementation usually is a change-management problem, not a technology problem. Put major projects under general managers with good political skills who can authoritatively deal with organizational conflicts and budget issues.
- **Improve budgeting and financing for promising IT initiatives.**
Explore budgeting options such as capital funds, revolving funds or shared-risk investments with the private sector that will allow investments in IT initiatives without relying too heavily on traditional government budgeting.
- **Protect privacy and security**
Do not misunderstand privacy and security issues, either by ignoring them or by allowing their volatile nature to paralyze development of new systems and services. Implement the fair information practices and secure information practices developed over the last 25 years, and stay ahead of controversy by early planning.

- **Form IT-related partnerships to stimulate economic development.**

Do not ignore opportunities to cross traditional boundaries in developing information technology projects. The biggest IT benefits often require cooperation across traditional boundaries between agencies, between state and local governments and between private industry and the public sector. Cross-boundary relationships can be difficult, but they are crucial to effectively develop IT possibilities in economic development.

- **Use IT to promote equal opportunity and healthy communities.**

The “digital divide” threatens to widen the gap between poor and wealthy communities. Leaders must address these issues carefully, neither ignoring them nor trying to develop massive programs that are doomed to failure. Focus on the kinds of net-based education, job development and community engagement activities that can be developed judiciously.

- **Prepare for digital democracy.**

The Internet has steadily shrunk the “global village,” creating many difficulties for policy makers and regulatory agencies. Networking that reaches across regional and national boundaries creates a question of what policies should be created and how they can be enforced. In the face of technological growth, isolationism is no longer an option. Instead, we must develop new initiatives to broaden the participation in rule-setting and enforcement issues.

Technology issues often seem complex and technical, so it is tempting to just leave technology to the technicians. But so much of what government does today is based on technology that we must get involved, both in developing it and keeping it secure from both casual and committed adversaries in the cyber-world.