IT's Role in Homeland Defense

Phillip J. Windley, Ph.D.
Chief Information Officer
Office of the Governor
State of Utah

Recent events have made it clear that we must protect ourselves within our borders as well as without. "Homeland defense" has become a common phrase, not only in Utah, but around the country. The question naturally arises as to what role IT plays in homeland defense. I think it is instructive that the second person Tom Ridge (Director of Homeland Security) appointed on his first day on the job was a deputy for cyberterrorism.

While IT has an important role in enabling public safety and citizen efforts in homeland defense, this article will focus on what roles we all have in protecting the informational assets for which we're responsible from intentional destruction or misuse. At the same time, most of what we do to defend ourselves from intentional abuse will also protect us from disasters of other kinds.

Production Data

In order to formulate a coherent and effective strategy for protecting IT resources from natural and man made catastrophes, we need to define what we mean by "production data." In a general sense, production data is data that is necessary to carry on the business of the agency. Production data comprises the databases or file sets containing an organization's master and daily transaction files that are used to process an organization's daily work.

Production data constitutes one of the most valuable information resources that belong to the State of Utah. Lack of access to production data can cause inconvenience, delay, and, in many instances, irreparable harm to the State. Such data must be protected both physically and electronically. Provision also must be made for recovery in the event of a disaster or cyber attack on the State's information resources.

All production data in the state should have at least two people associated with it: the owner and the custodian. Sometimes these are the same people, but often they are not. The owner is the person who is responsible in the legal sense for the creation, protection, use, archiving, and ultimate destruction of the data. This might be the agency or division director or other business line manager. The custodian is the person charged by the data owner with the day-to-day care of the data. This might be a subordinate, someone in the IT department, or even an outside contractor.

Data Security

One of the fundamental ways of providing protection to production data is to use industry best practices in establishing good data security. If designed correctly, good data security measures protect data from being stolen, altered, misused, or destroyed. Effective data security is difficult to achieve because it both must allow data to be readily available to people with a legitimate need while also being inaccessable to others who do not need to see it. Effective security must be balanced against optimal user convenience and that always requires trade-offs.

The first line of defense in data security is good physical security. No computer can be protected from compromise when the attacker has physical access to it. Production data should be stored in a physical facility that provides a controlled temperature environment, redundant backup power, automated fire suppression, 24x7 server monitoring and reporting, and restricted access controls compliant with Federal Guidelines for C2 level security.

The network is the most likely means of unauthorized access to production data. Because many of the computers we use everyday to do our jobs must be connected to the state network to function effectively, attackers can use the network to gain access to sensitive yet vital data.

Thus far, we have taken several steps to limit access to the state network from outside:

- We limit the Internet connections to state network to those provided through ITS. No other connections to outside networks are allowed without specific approval of the CIO.

- We limit outside access to state computers to a set of identified hosts for certain services using firewalls. We have more to do in this area, but we have made a start.

- I have asked IT Directors and ITS to move all computers accessed from outside the state network into a special security zone on the network that we refer to as a DMZ. All production data will need to be moved behind this zone and not reside on computers accessible from outside the state network.

These steps are necessary because many computers and other devices attached to the network (such as printers) contain web servers (and other network services) that are enabled by default and insecure. On the other hand, web services cannot be effectively filtered since they are frequently used for legitimate purposes. A DMZ places all web servers that can be legitimately accessed in a place where they can be monitored and all those that should not be accessed by the public in a protected area.

ITS has developed a security plan for computers that can be reached from outside the state network and that plan has CIO approval. Also, we must know about all connections to the Internet from the state network so we can take appropriate security measures to protect our vital assets.

Owners and custodians are responsible for ensuring that production data and the computers that process it are secure and meet best industry practices for computer security.

Intrusion Detection

One of the most difficult aspects of data security is protecting data from unauthorized access or outright destruction from intruders who enter via an authorized network connection. Intrusion detection is the process of actively searching for unauthorized access to data.

Intrusion detection is comparable to having security guards checking ID badges to ensure only authorized persons are allowed entry to restricted space. Intrusion detection is the process of scanning connections to web servers and other network services and looking for patterns of activity consistent with unauthorized use.

Intrusion detection involves more than just searching for malicious activity. It also includes responding to those threats in a credible way. The State of Utah employs intrusion detection on our connections to the greater Internet. When an intruder is detected, steps are taken to close off a service, block the address of intruder, or otherwise protect state assets.

Data Protection and Recovery

Anyone who uses a computer has heard about backing up their data to protect themselves from damage to the computer or its components and the subsequent lose of data. Most of us have also lost important data either due to faulty hardware, buggy software, or user error.

While almost everyone understands and acknowledges the need to effective back-up and recovery procedures to protect against unintended data destruction, few people have good or consistent strategies to carry it out. Fortunately, in today's networked world, much of the data back-up and recovery process can be done through the correct use of networked storage and a central group of IT professionals who are given responsibility and authority to ensure that this happens.

Business Resumption Strategies

One of the most important lessons from the recent tragedy of September 11th, is that events can and do occur which can destroy an organization's primary data services and facilities. The question that we must all ask ourselves in light of that

tragedy is whether or not we have a strategy for continuing to serve our customers and constituents in the event such a catastrophe struck our organizations. For some of us, I suspect, that the answer to that question is "no."

Business resumption strategies constitute a full plan for continuing to provide vital services following a disaster. The plan needs to take into account which services are vital, how those services are delivered now, and to what extent and in what manner those services would be available following a disaster.

Once services and functions have been inventoried, planning must be done to determine how best to provide redundant infrastructure to support those services. The level of redundancy and how best to achieve the required reliability is dependent on the service and the level of availability appropriate to the service. Clearly, providing redundant infrastructure for everything can be prohibitively expensive, so prioritization and upfront planning are necessary to limit the cost and provide vital services in a reliable and efficient manner.

In addition to planning for recovery of data and systems so that you can continue to offer vital services, you should also pay attention to critical job functions. Your most critical employees need alternate ways and places to work. You should plan in advance where you will find additional workspace (including desktop computers, network access, telephones, and email), prioritize critical job functions and employees, determine how you'll communicate with employees during and immediately following an emergency, and equip key employees to work remotely.

The State of Utah has invested significant resources in building the infrastructure that is necessary to support line of business resumption strategies by state agencies. That infrastructure includes a duplicate data center in Richfield with the full capabilities and features of the data center in Salt Lake, redundant, high speed network connections between those facilities and the rest of the state network, and processing capabilities in both locations. In fact, we do not simply use Richfield in the event of a disaster, but a portion of the state's daily processing is done there on a routine basis.

The investment that the state has made in this area will not do any good if agency business managers neglect to form business resumption strategies that will take advantage of the state's existing infrastructure. Many agencies developed business resumption strategies as part of their Y2K planning. Now would be a good time to review those strategies and ensure that they're up to date with regard to changes in lines of business and the IT infrastructure that supports them.

eGovernment

One of the lessons from September 11th is that government web sites were relied on by large numbers of people to find information, contact officials and even family members, and to gain access to vital services. Many government web sites experienced ten times their normal traffic immediately following the

attack and have sustained higher than normal traffic since that time.

After a disaster, the Internet often works when other forms of communication do not. Almost immediately following the September 11th disaster, up to 20,000 New York City employees were without phone service. As a cascading effect, cell phone circuits became saturated making most of these devices useless. Nevertheless, New York City was successful in part because it did not hesitate to re-deploy personnel resources to make sure information was continuously being supplied and updated via NYC.gov.

When the Salt Lake area was confronted with a recent disaster, a tornado, cell phone communication in the Salt Lake area was likewise rendered an ineffective communication tool in many areas. Unfortunately, unlike NYC, state websites, for the most part, were not well prepared to serve citizens during that emergency.

As we move to put more and more government services online, we also need to be aware that people will come to rely on them and turn to the Internet in times of trouble even when they haven't done so before. As we plan eGovernment services, we need to ensure that those services are not only secure, but also that they will be available in times of need. The state has the infrastructure and experience necessary to create high availability services, but we must plan from the beginning to build services that will sustain attack and natural disaster. This planning must be followed up with regular capacity planning to ensure that we can service the requests that will be made during an emergency.

Action Steps

What can you do to protect IT resources from harm and ensure that they are available for use when needed? The following list gives a few ideas:

- Inventory and identify critical lines of business and their associated data.
- Identify the data owner and custodian for each production data set.
- Ensure that your agency security policy is in line with the state security policy and that all production data is being adequately protected.
- Take steps to provide for the physical security of data resources and provide or use data center facilities that meet the minimum physical facility requirements.
- Set up ways to detect intruders on production systems and monitor them carefully.
- Ensure that all production data is being properly backed-up and that it can be recovered in the event of catastrophic events.
- Prepare a business continuation strategy for each line of business and review it frequently to ensure that it remains current in the face of changing business requirements. Dust off your Y2K plan and turn it into a living document for business resumption planning.

- Practice and drill your data recovery and business continuation plans. This strategy saved the NASDAQ and allowed the financial markets to come back up within a week of the September 11th attack.
- Engage in regular capacity planning on your agency web site to ensure that you have sufficent excess capacity to service citizen needs in an emergency.
- Plan how you will update information on your agency web site immediately following and throughout an emergency to communicate with citizens and others who you may not be able to reach in any other way.

If you need to know more about IT resources inside the state to support your efforts, please contact your agency IT Director or Rick Gee in ITS.