Dec. 2001
Vol. 1 Issue 7

Powered by

IT Security :
Protecting Iowa's Infrastructure

Security is now a big deal. The more technologically savvy we become - in government and society - the greater the need for sound digital security operations. This urgency becomes even greater as digital technology grows more entwined with our "backbone" resources such as transportation, finance and energy.

With the expanded Enterprise Information Security Office, ITD's in-house security team can better address information assurance from an enterprise perspective and provide security assistance to state agencies. This expanded service results in monetary savings for taxpayers by reducing the need for high-priced outside security consultants.

"We operate systems that store, process, transmit and receive information vital to the citizens of Iowa," says Kip Peters, chief IT security officer. "We have the responsibility of protecting that information - we are the caretakers. With the inherent security problems in today's systems and the multitude of existing threats, we would be grossly negligent to not protect that information and our information systems."

The Security Office has embarked upon several projects essential for a comprehensive information assurance program. They include:

- Formulating an Enterprise Security Policy, currently in working draft form.

- Developing a suite of services available to state agencies and other Iowa governmental organizations. Services include security consulting, system/network and physical vulnerability assessments, intrusion detection and incident response.

- Devising an enterprise security awareness program to inform government computer users on security issues. The program includes a Lunch & Learn series, weekly Security Quickies, the Security Blanket (the Security Office's monthly newsletter), and an upcoming security awareness Web training application. The Security Office also distributes information on vulnerabilities and patches, alerts, and issues to the technical community.

- Implementing a security test lab, which is available for testing new products and machines, upgrades, patches, and standard configurations.

Security - *Continued from p. 1*

- Researching better identification for computer users via biometric authentication, public key system or other identity security measures.

- Helping establish an InfraGard chapter in Iowa. InfraGard is a five-year-old partnership between private industry and the U.S. government (represented by the FBI) to encourage the exchange of information between government and the private sector to counter cyber and physical threats.

- Developing a web site (*http://www.itd.state.ia.us/security*) containing security information of all kinds and updates on the activities of the security office. It includes policies, guidelines, presentations, streaming video of past Lunch and Learns, current service information, contacts, and links to other resources. Up-to-date security information for users of the AvantGo service for personal digital assistants (PDAs) is available and the news is updated twice weekly. It contains ITD news, Microsoft vulnerabilities and virus information.

- Collaborating with the Division of Criminal Investigation computer crime investigator on issues involving computer compromises.

- Establishing a partnership with Iowa State University's Information Systems Security Laboratory and Information Assurance Center. Also ITD Security is consulting with Iowa State on its new Masters program in Information Assurance.

The Security Office was also instrumental in enhancing Iowa's critical infrastructure assurance through a partnership with the Emergency Management Division (EMD) of the Department of Public Defense.

Critical infrastructures are those vital to the daily lives of Iowans and their economic well being. They include telecommunications; electric power; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services; and continuity of government.

During the past year the Security Office with EMD:
- Hosted a Cyber Terrorism seminar for personnel associated with Iowa's critical infrastructures. The event attracted statewide personnel from all eight critical infrastructures.
- Assisted in developing the National Plan for Critical Infrastructure Assurance.
- Presented Critical Infrastructure Assurance issues to some Iowa counties.
- Commissioned a study on Iowa's transportation systems.
- Participated in identifying and conducting a risk assessment of Iowa's critical assets.

> *During recent Code Red attacks not a single server monitored by intrusion detection sensors was infected by the worm, while other servers not monitored were infected.*

The team analyzed an average of 650 alerts each day during FY 2001. Numerous attempted attacks were identified and serious consequences were prevented because the appropriate system administrators were alerted and problems solved. During recent Code Red attacks not a single server monitored by intrusion detection sensors was infected by the worm, while other servers not monitored were infected.

Currently, the team is developing its own intrusion detection sensor at a fraction of the cost of commercial sensors. If continued testing and development goes well, the use of in-house sensors will save the state a significant amount of money. The Security Office is also working to be more proactive than reactive. Some FY 2002 goals and objectives are:

managing IT

- Vulnerability assessments of all state agencies.
- Assisting each state agency in conducting an agency risk assessment.
- Enhancing Iowa's critical infrastructure assurance and establishing a statewide critical infrastructure assurance working group.
- Offering biometrics usage for authentication purposes within ITD, pending budget availability.

"Security is not an exact science, and it's not a goal or state of being. It's a process," points out Peters. "It's something that must be considered continuously and acted upon. Perhaps the one word that best describes security is diligence - we must be vigilant, thorough and careful. Without those, nothing else matters." For more information, please see the Security Web site or direct inquiries about security assistance to Kip Peters directly at 725-0362 or Kip.Peters@itd.state.ia.us.

Staff reductions at ITD

As a result of FY02 budget reductions, approximately 9% of ITD's total staff from the operations, customer liaison and administration divisions were laid off.

In order to mitigate the number of full-time, permanent job cuts, a majority of ITD interns, probationary employees and some outside contractors were released. In addition, ITD continues to identify ways to reduce operating costs.

While customers may experience delays in project completion or responses for service requests, be assured that ITD remains committed to serving customers and is working to minimize the impact of a reduced staff.

The **Council** for Sage **Counsel**

For more than 20 years, several organizations have served a similar function for state government - providing a way for information technology professionals to gather and share information. The group currently known as the Chief Information Officers (CIO) Council promotes policies and practices for effective use of information technology for the State. Prior groups have been known as the Information Technology Management Committee (ITMC); Information Management Committee; Telecommunications and Information Management (TIM) Council; and the Communications Advisory Council (CAC).

With the launch of ICN and ITD, the need emerged for better communication between those entities and the users of their services. The CIO Council is one vehicle.

"In most cases, it's not convenient or efficient for information technology representatives from various state entities to deal with issues on an individualized basis," says Leon Schwartz, IPERS chief operations officer and CIO chair. "There's value in having the capacity to hear what other agencies have to say. By having an organization to assist those responsible in government for achieving efficient use of these resources, collaboration among all members of the state enterprise is achieved."

An example of such collaboration occurred during a recent Return on Investment (ROI) analysis of technology project funding requests with the Iowa

Information Technology Council (ITC). The ITC is the Governor-appointed oversight body for the Information Technology Department. Because ITC wanted consolidated feedback, they received one score from ITD staff for each ROI and one score from the Council. The Council ranked all of their peer's projects and gave that score to ITC. The score reflected what the council as a group felt about those particular projects. If ITC had gone to each agency separately they would have received some feedback but without the added value of cross discussion and sharing of information within the Council. Also, it would have taken considerably longer to get to the end result.

CIO Council input will be needed as the state moves to consolidate a variety of decentralized IT functions among state agencies—including email, Web hosting, data warehousing, storage area networks and server management—into a more cost efficient, integrated and centrally administered system.

A purely volunteer group open to all State of Iowa government organizations, the Council is exempt from the open meeting policy and doesn't have legislative authority. The Governor selects its chair and the vice-chair is selected by the Council.

"It's a coordinated activity simply because a group of individuals recognized the need to talk among themselves while also communicating with service providers," states Schwartz. "Most importantly, it maintains relationships and ensures communication with the ITC, ITTC, ITD and ICN

3