Washington Computer Incident Response Center – Security and Business Continuity

Title of Nomination: Washington Computer Incident Response Center (WACIRC)
Project/System Manager: Darlene Kosoff
Title: State Security Manager
Agency: Department of Information Services
Department: Enterprise Security Services
Address: 605 East 11th SE -
City: Olympia
State: WA
Zip: 98504
Phone: 360-902-3253
Fax: 360-586-3595
Email: darlenek@dis.wa.gov
CATEGORY: Security_and_Business_Continuity
Person Nominating (if different): Stuart McKee
Title: Director, Department of Information Services
Address: 1110 Jefferson Building
City: Olympia
State: WA
Zip: 98504
Phone: 360-902-3500
Fax: 360-664-0733
Email: stuartm@dis.wa.gov

Executive Summary

The past 10 years have witnessed a 50-fold increase in electronic traffic between the Internet and state and local government networks. This traffic must be protected to maintain citizens' trust in government. However, incidents such as virus and denial of service attacks constantly threaten to shut down private and public sector businesses alike. Washington state's ongoing priority in the network security arena is to protect the state's assets and keep government business operating around-the-clock.

On November 21, 2001, in a letter to the State of Washington Information Services Board (ISB), Washington state Governor Gary Locke, announced a new anti-terrorism measure enactment to:

- Establish standards for ensuring the security of state technology, including the physical security of computers and telecommunications and anti-virus protection;
- Establish standards for the connection of computers to the state network and the circumstances under which they will be terminated and restored;
- Facilitate the sharing of security information, tools, techniques and methods among state agencies;
- Foster cooperation among state agencies for the effective prevention, detection, handling and recovery from technology-related security incidents, and
- Establish an Incident Response Center within the Department of Information Services (DIS), and a process for reporting computer security-related emergencies and the communication of alert and advisory information about security threats and incidents.

At Governor Locke's direction, DIS established the Washington Computer Incident Response Center (WACIRC), a collaborative partnership of authorized state agency security professionals who work together to establish a strong security defense strategy for the entire state government network and to provide continuous business continuity of services while protecting against new cyber threats that aim to infect government systems.

On April 12, 2002, WACIRC adopted its mission "to establish processes for reporting and responding to computer security-related emergencies and for the communication of security alert and advisory information."

WACIRC is not intended to replace existing agency or organizational computer security response teams. Its goal is to serve as the focal point for agencies to report and communicate information about computer-related security incidents. WACIRC and associated partners participate in a cooperative sharing of incident-related information, statistics, trends and best practices.

DIS promotes participation in WACIRC, recognizing that the "chain" of state security and business continuity is only as strong as its weakest link. This membership's goal is to support enterprise-wide security with two-way communication through a central WACIRC incident-reporting portal. Information on security-related incidents or weaknesses that are collected by each individual agency without communicating that information to other members fails to provide any value to state government as a whole. Collaboration around such information is the foundation of a strong defense strategy for the entire state government information infrastructure. WACIRC has changed the incident response model from a model of merely responding – to a model of two-way collaboration of incident reporting, sharing, responding, containment and recovery. This first-of-a-kind approach has already proven itself multiple times with not only scheduled cyber exercises but also real-time incidents such as SLAMMER. The state is achieving its goals in WACIRC through effective prevention, detection, containment, eradication, recovery, lessons learned from technology-related security incidents and recommendations for effective improvement.

The key is ***rapid response to security incidents***. Once an incident is discovered, every second that passes is critical to the protection of the state systems. Rapid response is key to heading off cyber tragedies in government networks. This can only be done through a collaborative spirit and formal process of state agencies working together.

WACIRC uses the following strategies:

- Invests in infrastructure capacity and resiliency
- Protects mission-critical business with data network security
- Invests in continuous availability and Web-readiness for computing systems.

Washington Computer Incident Response Center – Security and Business Continuity

The significance of this approach and implementation cannot be overstated. It is paramount to the prevention, detection, containment, eradication, recovery and lessons-learned strategy within Washington state. Washington state government is stronger by joining together forces to deal with security incidents.