Technical Panel
of the
Nebraska Information Technology Commission

Security Architecture
Incident Response and Reporting Procedure for State Government

COMMENTS RECEIVED

COMMENT #1 Ron Woerner

To whom it may concern:

I have two comments on the Draft Incident Response and Reporting Procedure for State Government:

1. Ensure that only true security incidents are reported. In my experience, most "incidents" turn out to be either mistakes or misunderstandings. In the first case, a user or administrator will accidentally take down a system. While end users may see that as a denial of service attack, in reality it's not. In the case of misunderstandings, I've seen one administrator make a system change and not communicate it. Someone (either a user or admin) stumbles on the unexpected change and calls in an incident. I do not consider either case to be a security incident, but they are both often reported as such. I have seen a lot of time and paper wasted investigating such incidents. I believe it is important to communicate that true security incidents involve either malicious intent or intent to go around the system. Lack of communication should never be the "Nature of the Problem."

2. In any government organization, retaliation for malicious activities (i.e., intrusions, DOS, probes, etc) should not be allowed. The SecurityFocus article "Appropriate Response: More Questions Than Answers" (found on-line at http://www.securityfocus.com/infocus/1516) describes two types of individuals that respond to security incidents: Defenders and Digilantes. Defenders "follow policies with a primary emphasis on preventing breaches in the first place. If there is an intrusion, a Defender focuses on containing and eradicating the problem, plugging the security hole and getting back to business." "On the other hand, Digilantes, or digital vigilantes, have no qualms about striking back against attackers." I believe this policy document should state that government employees or contractors are not permitted to strike back against attackers. The appropriate authorities should handle all punitive actions.

These comments are strictly my opinions and do not necessarily represent current or future employers.

Ronald Woerner, CISSP

TECHNICAL PANEL RESPONSE: