SSAC
ICANN Security and Stability
Advisory Committee

23 April 2008

SAC031: SSAC Review of the After Action Report for the gTLD Registry Failover Exercise conducted 24-25 January 2008

SSAC thanks ICANN's Registry Liaison Manager & Coordinator for the opportunity to review the above mentioned report (see http://www.icann.org/registries/failover/). We believe this exercise and the Registry Failover Planning process itself are extremely important activities and support current and future studies of this topic. This is important work, an important step for ICANN and existing registries, and one that ICANN ought to complete before it begins the new GTLD process

Our comments on the report follow:

1. We would like to see an increased emphasis in the visible and critical role public relations (corporate communications) plays in representing incidents to not only the public, but to regulators, business partners, and governments. This is mentioned in Observation 4 in the report, but it is not addressed in more detail in the main report. Security professionals consider disclosure to be a key component of incident response and resolution and consider "disclosing badly" a potential incident itself.
2. Page 10 mentions "achieved internal and external coordination points during crisis response..." This statement is confusing and requires clarification.
3. Page 11 mentions "communications during an event" but does not make clear whether these communications are internal, external, or both. Many DNS events at the registry level will be sufficiently visible to require internal *and* external communications. We believe that ICANN must consider and document its role in registry failure scenarios includes "buffering": communicating with the press, reassuring the public during an ongoing investigation, reporting or providing testimony to regulators, and other, similar incident related activities.
4. On page 12, second recommendation, we believe it would be helpful to explain that Incident Response is a chronology of events that begin with notification, detection or reporting; continue with assessment and disposition (dismiss or escalate); continue further with analysis, response, and resolution; and conclude with post-incident assessment, review and revision (if needed) of policy/procedures.
5. On page 12, "information sharing" is used loosely, without explaining the parties among whom the information is shared among.
6. Page 12 mentions Denial of Service attack monitoring. We assume this statement refers to monitoring TLD registry name servers; however, it's not clear whether the monitoring discussed here is a real time traffic analysis or an out of band notification system. SSAC believes that real time monitoring would be a very large scale activity

if implemented today, and notes that the activity would grow quickly with the introduction of new GTLDs.

7. Certain events may not escalate to a crisis condition. The nomenclature "Crisis Response Team" biases parties into concluding that an event is always a crisis situation. If possible, we would suggest you find an alternative name for the team.
8. Observation #3 calls attention to ICANN's dependency on individuals rather than roles. This is a problem in many organizations and we commend ICANN for acknowledging this as an issue it must address. Under recommendations, we would like to see ICANN commit to developing clear, role-based process flows and responsibilities. The documentation for such flows could be modeled after a trouble ticketing system, and should identify means of notification, information that must be transmitted, response window, etc.
9. On page 14, under initial event investigation, we believe the plan should *not* identify an individual (this is the problem discussed in item 8). Incidents should follow a defined flow, through individuals whose **role** is to manage a particular aspect of the flow.
10. On page 15, the external contacts list is largely populated with operational contacts. Non-operational contacts - press, regulators, government agents, law enforcement - should be identified by corporate communications and included in this list. Also, this section should task ICANN with identifying not only who is contacted, but **when** and by whom.
11. Under Observation #5, we believe it would be helpful to distinguish the several possible cases of transition:
    1) Temporary (transitional). Some party takes over until a full time operator is identified.
    2) Permanent. A full time operator enters into a contract with ICANN to run the registry.
    3) "no takers". No full time operator steps up (the registry is a bust) and the temporary operator wants to terminate its support (or the money runs out)

    Observation #5 implies that a transition will always occur. We would like confirmation that this will indeed always be the case; specifically, we speculate whether there will be situations where the cost/benefit analysis does not justify a transition. For example, suppose a new GTLD exhausts its investment capital, cannot find additional funding, revenue is insufficient for the registry operator to remain in business, and the registry has a few dozen or hundreds of registrations. This may be an outlying situation, but we ask whether the plan should consider it..
12. On page 16, We do not understand what is meant by "neutral" holding facility. Specifcally, we do not understand who judges the facility to be "neutral".

____

Dr. Stephen Crocker
Chairman, Security and Stability Advisory Committee