Missouri Information Security Incident Response Plan

Executive Summary

As an integral part of the comprehensive security program for the State of Missouri, the Information Security Management Office (ISMO) in the Information Technology Services Division has developed and implemented an Information Security Incident Response Policy and Plan. This five step plan encompasses everything from the end user responsibility to the State Chief Information Officer's coordination with the elected officials. It is imperative that the State's Information Technology community is aware of and trained in dealing with information security threats to minimize the damage from security incidents and malfunctions. A comprehensive Incident Response Plan was implemented to address issues as emphasized by the Governor of Missouri in an Executive Order to Missouri state agencies:

WHEREAS, cyber attacks seek to threaten public safety, individual privacy, corrupt valuable data, and disrupt the capability of public and private entities to function effectively, thereby eroding public confidence; (Missouri Executive Order 03-25)

As data owners and custodians with statutory or operational authority for specified information and the responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal, the state is bestowed with the responsibility to protect citizen's data from unauthorized disclosure, manipulation, and fraud.

An information security incident is an adverse event where an agency computer resource is accessed or used without authorization, attacked or threatened with attack, or used in a manner inconsistent with established policy. These incidents have the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information. The data compromise or severity of the impact determines the level of response.

Incident severity levels are a value assigned to an incident based on its potential to negatively impact agency operations or an agency's public image. The incident levels applied in this process, mirror the color and numeric escalation as prescribed by Homeland Security Presidential Directive-3 and are illustrated in Figure 1.

The methods described in the Plan for responding to breaches of data from malicious activity and securing privacy continues with specific steps that combine the efforts of analysts and technicians to quickly halt malicious activity. Care is taken to ensure investigative information is collected and maintained in a manner that is consistent with the means to prosecute offenders. A review of every incident is conducted to identify any area that could be improved from lessons learned during the investigation. This system of reporting, declaration and notification, investigation and containment, resolution, and follow-up combined with training and communication, provide the citizens of Missouri assurance that any attempt to breach the security protecting their information will be met with concerted efforts to halt infiltration.

Business Problem

Agencies work diligently to keep their own networks and systems free from viruses, bots, and the impending security breaches waiting to launch. Each was working to protect the data and keep their local area network secure and fulfill obligations to protect the privacy of those whose vital information is stored and transported via state's network.

While this was a valiant effort, it was a narrow effort. All agencies share the same state network. Even though there are firewalls and detection devices protecting us, once on the state network, isolating an attack becomes more complicated. The threat to public safety, individual privacy and valuable data explodes.

Without a methodology that is consistent throughout the agencies, precious time was lost while individual agency staff members struggled to contain the incident. During this time, information was being lost or corrupted and vital services were interrupted. Without a system to share information and expertise across agencies, perpetrators were free to duplicate their efforts on other unsuspecting agencies.

Solution

During the early months of 2006, Missouri finalized the policy and plan to standardize the methods used in the face of a security incident. The documents were vetted through the Information Technology Advisory Board, which is comprised of the Information Technology Directors from every Department. This vetting process guaranteed understanding and full cooperation from all Executive, Legislative, and Judicial branches.

The foundation for incident response is illustrated in Figure 1 with the transition from an event to an incident. The severity level of the incident determines the rigor of subsequent response paths and the timeliness requirements.

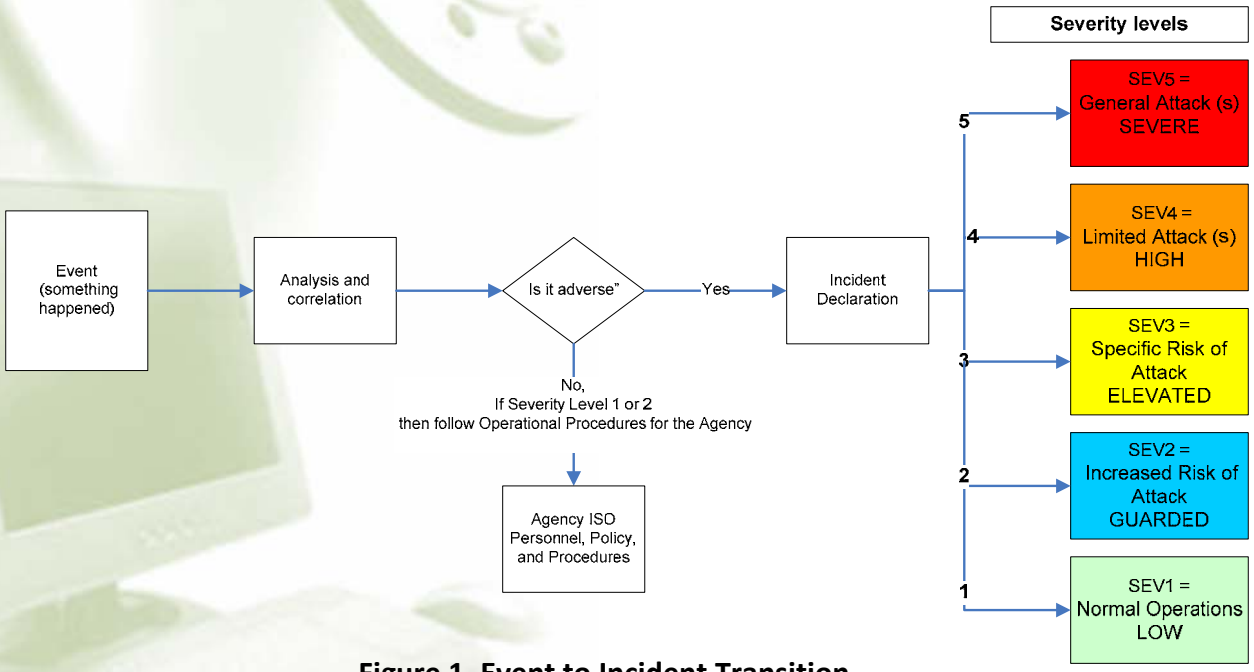

Figure 1. Event to Incident Transition

A high-level view of the flow process is illustrated in Figure 2. Although the process has a set structure for working through an event, it is also flexible enough to allow for responders to temporality bypass specific formalities if the situation presents itself as catastrophic in nature. The objective is to halt malicious activity as quickly and efficiently as possible. The needed documentation may be completed at a less hectic time. This in no way encourages skipping steps, merely building in flexibility when time is of the essence.

Communicate, communicate, and communicate. One cannot stress this enough. **Communicate** before an event to provide awareness so staff members know what to report. Training is conducted to promote communication and to set the foundation of awareness and trust. **Communicate** when responding to a breach to ensure all interested parties are aware of the situation, to procure assistance and be vigilant in other areas. **Communicate** when the event is resolved to better understand what went right and what went wrong. Much is learned by reviewing actions and reactions. Opportunities for reassurance and improvement will be realized. To minimize damage, agencies communicate and learn from each others experiences.

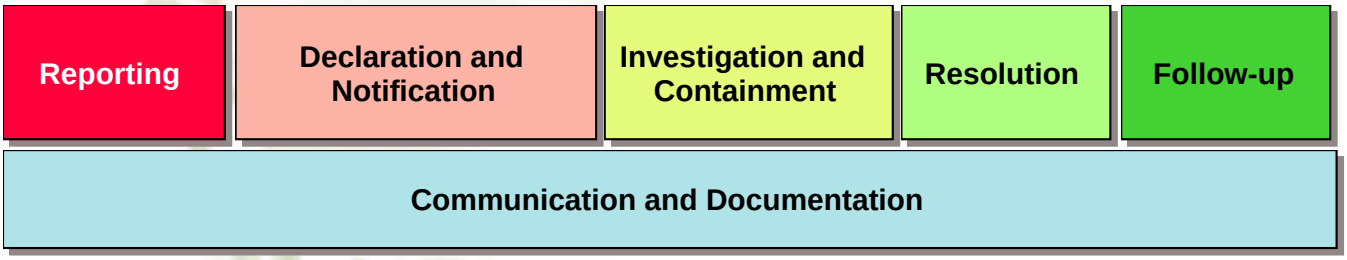

Figure 2. Incident Reporting and Response Process Steps

Project Description

This project was established to address the effective development and coordination with respect to information technology principles and governance; to work diligently to combat cyber attacks and to protect the cyber assets of the state. The establishment of centralized information security management teams capable of executing and supporting industry recognized security provisions, programs and assessments was paramount to the success of the Plan.

Any persons or agencies that must respond to, stop or contain an incident in progress or must restore a system affected by an incident are considered primary responders and play a vital role in the process. Secondary responders may also be those not directly involved with stopping or containing the actual event but assist with ancillary duties and responsibilities such as Fiscal, General Counsel, Human Resources and Public Information. All must work together with a common understanding of the means used to mitigate and halt malicious activity that threatens the security of protected data. Missouri's Incident Response Plan was designed to provide that common understanding and set of procedures for all to follow. Although the other information is paramount, the heart of the plan is the five reporting and response process steps. They were designed to be extracted from the manual and given to the group identified as responsible for carrying

out the specific functions described in that particular step. When an event is reported, that information is immediately captured and the overall process is set in motion. At each point, for each decision, the relevant instructions are provided and the path has already been clearly established.

Significance to Government Operations Improvements

To fulfill requirements requested by the Governor's Executive Order, the Incident Response Policy and Plan has become the standard by which all State of Missouri agencies report and respond to security threats.

Consistent formats for reporting and responding to security incidents is essential to Information Technology operations. This project provided policy and a plan consisting of procedures to raise the awareness of the security of the State's information community. Specific responsibilities were assigned to improve communications and outline tasks:

State Chief Information Officer (CIO)
Review and approve the Incident Response Procedures.
Brief Cabinet and Agency executives as required.
Direct the Public Information Officer to brief third parties as required.
Delegate authority for real-time, immediate response actions to the DIS, Agency IT Directors, and managers of the affected IT resource.

Director of Information Security (DIS)
Oversee the Incident Response Process execution.
Brief Cabinet and Agency executives as requested by the CIO.
Coordinate with the CIO and Public Information Officer on third party briefings.

Information Security Officer (ISO)
Provide or receive initial event report notifications to and from the Help Desk.
Track the findings of event analysts.
Provide situational briefings to the DIS and the Agency IT Directors.
Ensure contact information is up to date.
Execute the Incident Response Process on behalf of the DIS.
Brief the DIS and agency executives as required.

Agency Employees
Report events and assist the response team as necessary with their incident response activities.

Public Value

The value to the public is in what they do not see. That value being the absence of media reports of social security numbers, medical information, credit card and banking information having been stolen. There are in excess of 5,840,000 citizens in Missouri expecting the state to keep their personal information from unauthorized access or disclosure. The confidence of the citizens in the ability of the state to protect their

information allows for each to conduct business electronically, which provides for a faster, more cost effective method of service to the public.

Return on Investment

Every day brings another story of a system vulnerability being exploited, resulting in system downtime and economic losses. In the case of a security breach, time is the underlying culprit. Time is money and time is the continuing loss of data. Every minute that Missouri's network is interrupted approximately $36,000.00 dollars are lost. Every minute counts. There is no time to come up with a plan. There is no time to think about what to do next. What steps to take, what to expect and where to find assistance has been thought out and documented in the Incident Response Plan. These processes implemented consistently, across all agencies provide the early efforts needed to stop the loss of information before the damage is done.

Conclusion

Any event has the potential to become a security incident by compromising the security and integrity of sensitive and protected information. The fiduciary responsibility to stop an event resides with the state; from the Governor to the end-user. Missouri's Information Security Incident Response Plan as shown in Figure 3, provides a cohesive methodology to understanding and fulfilling the responsibility for information security.