Incident Response and Reporting

(How to Survive an Incident!)

FISSEA 2004

Tuesday, March 9, 2004

Tom Walsh, CISSP

President

Tom Walsh
Consulting, LLC

6108 West 121 Street ◆ Overland Park, KS 66209

Phone: 913-696-1573 ◆ e-mail: twalshconsulting@aol.com

Background

It's a fact of life: no matter how many precautions or countermeasures you take, a security incident will occur. The critical issue is how you deal with a security incident after it occurs. Are you confident that you are prepared to respond in a sound, methodical way or would you just muddle through and hope nobody notices? In this dynamic session you will have the chance to find out by testing your survivor skills in the wake of two incidents. You will view "documentary" presentations on the incidents and then face difficult decisions about what to do … and what not to do. This interactive format will provide an invaluable opportunity to see how you and your fellow peers would respond to a serious security breach … and let you walk away with pointers on how to improve your response. The session will end with a panel of experts weighing in on what they think are the best ways to respond to specific incidents.

Session Objectives:

- Explain the key steps involved in incident response
- Describe the process for properly responding to an incident
- Participate in security incident scenarios and determine the appropriate next steps in response
- Obtain advice and opinions from peers

Special "Thanks" to:

Troy Hottovy, Director, Information Security, and **John Wade**, VP and CIO, Saint Luke's Health System

Thomas Akin, Director, Southeast Cybercrime Institute, Kennesaw State University

Patrick Gray, Manager, X-Force, Internet Threat Intelligence Center, Internet Security Systems and former FBI agent

Eric Maiwald, Chief Technology Officer, Fortrex Technologies, Inc. and co-author of *Security Planning and Disaster Recovery*

Disclaimer:

The names and events depicted in the scenarios are fictitious.

Conditioning Our Responses

- Drills, exercises, simulations, tests –
  Condition us for automatic responses.
- Why?
  - To increase our chances for survival!
- In a crisis:
  - We do not always think and act logically
  - We get too wrapped up in the event to remember everything we need to do

Definition of a Security Incident

A ***computer security incident*** is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

NIST Special Pub 800-3

Establishing a Computer Security Incident Response Capability
by John P. Wack

Major Causes of Incidents

- Unintentional or intentional actions of workforce (employees, contractors, vendors)
- Hackers: Denial-of-service attacks
- Malicious code
- Environmental: Loss of power, fire, flooding

The best way to make a security plan: Prepare for all the things that could go wrong and figure out how you'll deal with them.

Incident Report and Response

Goals:

- Identify
- Contain
- Correct
- Prevent

One of the maxims of security is,
"Prevention is ideal, but detection is a must."
--SANS Institute

Some things to remember when at the scene of an incident:

The damage to your company's reputation may outweigh the financial loss of the damage caused by an incident

Scenario #1 – Fire in the Hole: *Missing in Action*

One of the biggest concerns in a Data Center is the loss of operations due to a fire. With all of the organization's mission critical systems concentrated in a single room, Data Centers are not only vulnerable to fire damage, but the hazards and problems associated with fire suppression and clean up.

Exercise:

Describe what you believe should have been first five the key steps in responding to this incident.

1.
2.
3.
4.
5.

Describe what Bill should have done to document and respond to the missing backup tape.

Scenario #2 – Healthcare Worker Associated with Burglaries

On the surface, an incident may appear to be a simple open and shut case. However, without thorough investigation and proper follow up, it could turn out to be disastrous for an organization's reputation. The title of this scenario could have easily been the headline in a local newspaper.

Exercise:

What evidence should have been collected and how should the evidence be handled?

Describe your ideas for properly handling the local news media and other publicity.

Describe what steps could have been taken to ensure a third party that houses your data is a partner in such a response.

Incident Survival Tips from the Experts

Before the incident:

1. Identify your Incident Response Team (IRT). Consider including the following folks on your team:
   - Incident Response expert (Typically the Information Security Officer)
   - Technical Staff – System administrator, network administrator, etc.
   - Executive Management
   - Legal Counsel
   - Physical Security
   - Public Relations
   - Human Resources
   - Law Enforcement (if necessary)
   - Head of the section/department that had the incident
2. Define the authority of the IRT.
3. Identify the organization executive to contact for actions outside of the authority of the IRT. (This may be you Public Relations person.)
4. Define a standard set of procedures to determine if an event is or is not an incident.
5. Define a standard procedure for investigating an incident and the procedures for collecting and preserving evidence.
6. Provide formal training for your IRT. You may want to consider doing an announced and/or an unannounced test of your incident response procedures. Training your IRT will give them confidence in responding positively to incidents.

During an incident:

1. Don’t panic and get wrapped up in the excitement!

   To successfully handle an incident, you must remain calm and respond. Quickly try to get a handle on the situation and control it.
2. Take good notes.
   Maintain a set of notebooks to allow documentation during an incident. Give each member of the IRT a fresh notebook to write down what happens during the incident. Take detailed and complete notes. You may need them later as evidence if there is legal action as a result of the incident. Be sure to get your facts straight.
3. Pull in additional help if necessary.

   If you have no clue what to do--don't wing it! Unplug the system from the network, and call in an expert.

4. Control the information about the incident.
   ”One of the hardest things about handling an incident is enforcing the "need to know" policy. Incidents can easily be misdiagnosed early on. Things are not always as they seem, especially where computer security is involved. Keeping quiet about an incident ensures that you won’t be quoted in the press saying something foolish. Keep in mind that if an incident turns out to be significant, there is always the chance of legal action.” – SANS Institute

5. Contain the incident.
   If you suspect that a system has been hacked, then isolate it from the network. Collect evidence and protect it following these tips from SANS Institute:
   - Identify every piece of evidence with a witness.
   - Sign, seal and date a copy of everything.
   - Place everything in a tamper-proof locked place that only a very limited number of people have access to (and be able to prove only a limited number of people have access).
   - Sign, seal and date a copy of everything.

6. Correct the problem and get back to business.
   Use your backups, disaster recovery and contingency plans to help you return to normal operation.

After an incident:

1. Hold a post-incident meeting.
   Determine what lessons were learned and how you and your team could improve your incident response.

Follow these tips – and you’ll improve your chances as a “real survivor.”

