

## PERFECTING INCIDENT RESPONSE

C. MATTHEW CURTIN, CISSP

JANUARY 16, 2009

Many organizations now have plans for handling “incidents” in their organization—a loss of confidentiality, integrity, or availability of an important resource. How well those plans will work, though, is anybody’s guess.

### *Drilling Your Incident Response Team*

Not only do you need the technology, people, and processes in order to respond to an alarm; your organization has to understand how to work through a situation, how to think on its feet when things aren’t exactly as expected. When you’ve got a credible threat against a major asset, you don’t have time for learning along the way: you need execution.

Intuitively we understand how a plan can be well-executed: we practice. Athletes practice their games day in and day out, watching their performance, and modifying their strategies and tactics to improve. Nobody wins on game day without going through the exercise.

Incident response teams are no different from other teams that have a need to move quickly into the mode of execution. An incident response team that has worked together and understands how to deal with events as they emerge is one that can work effectively to identify, to contain, and to remedy incidents—even under pressure.

### *How We Drill*

Interhack’s Incident Response Team Drills work by working with you to develop a scenario that makes sense for your organization. Your experience in handling incidents, the type of information that you manage, and the incident activity actually taking place in your industry<sup>1</sup> are all considered.

The drill itself can be conducted at your facility or an offsite location. As your team goes about its work, our Red Team begins

#### Incident Scenarios Include:

- Live attacks;
- Regulatory actions;
- Sensitive data breaches; and
- Litigation and e-discovery.

<sup>1</sup>.

the scenario. Your staff then goes about the process of identifying the incident, assessing it, and working toward resolution.

At the end of the drill, we debrief the teams, openly discussing the attacks used, the responses, and talking about surprises that we found. Any compromise not identified by the Incident Response Team is revealed by the Red Team and a discussion for how to identify such compromises ensues. The result of this discussion forms the basis for revising the plans, tools, and expectations around incident response handling.

### *Preparing Your Drill*

Developing a scenario for you is the first step of our engagement. To prepare yourself for how to choose a scenario, consider your organization's threat profile. What are the likely threat sources, and what kinds of threats are they presenting? Think broadly, including issues including both operational risks and problems in software and configuration but also issues that come up due to regulatory investigation, litigation, public records requests, or whatever else outside of your organization causes your organization to divert resources unexpectedly.

### *Why Interhack?*

Originally formed as an information assurance research group, Interhack has always worked to understand not just today's security concerns but how that will affect the needs for security tomorrow. Through our publications, presentations, and training, we have helped clients and other practitioners understand how to identify what is important and how to manage it with the right balance of risk, utility, and expense. For more information, see our Web site at <http://web.interhack.com/>, or call us for client references and to see how we can help your organization.

1. Use training drills to understand:
  - (a) How well-prepared organization is for the scenario;
  - (b) How well the organization executes its plans;
  - (c) How the response compares to other executions of similar scenarios by other organizations; and
  - (d) Where the organization can improve its planning and execution.
2. Make drills relevant by assessing threat profile (including litigation) to find:
  - (a) High-risk activities: Where likelihood or impact of failure is high;
  - (b) High-expense activities: Where expense is concentrated; and
  - (c) High-frequency activities: Frequent activities.
3. Prioritize followup activity based on findings by aligning performance with business priorities, e.g.,
  - (a) Reducing risk,
  - (b) Reducing expense,
  - (c) Reducing frequency of turning routine response activities into a "project" or
  - (d) Reducing response time.

Figure 1: Finding a Good Scenario