

# Be prepared by creating your own incident handling guide

There is no way to completely eliminate computer and network security risks. The most we can hope for is to minimize risks and be prepared for the day that something goes wrong. What do you do if that day arrives? You follow the steps laid out in your security incident handling guide.

An Incident Handling Guide (IHG) helps your organization respond to security incidents that range from improper use of company resources by employees to the theft of private customer information by a skilled hacker. It guides the organization's initial response to a problem, and it helps to protect evidence, individual employees, customers, and the organization itself. An incident handling guide isn't as technologically exciting as firewalls and intrusion detection systems, but it is perhaps the single most important corporate security policy or procedure document you can have. An organization without a security IHG is like a building without clearly marked fire exits. Without a clear, predefined plan, people can panic and do unpredictable things that could endanger themselves or the company.

## Answers to tough questions

Still not convinced? Consider the kinds of questions that might arise during a security incident:

- *I think our Web server might have been compromised.* Should I unplug it to prevent further exposure, or will I get fired for taking it down? Placing the burden of this question on a new administrator, alone on the night shift for the first time, is unlikely to always yield the desired outcome. An incident handling guide gives the administrator an answer to this question or tells her whom to call. Clearly, the procedure is different for a company with an informational Web site than it is for an Amazon, eBay, or Google, whose business depends on its Web presence. Taking down the informational site has minimal impact, while taking down an e-commerce powerhouse has significant financial implications. Your IHG helps determine what's right for your company.
- *I think we might have an incident.* Should I tell my boss, coworker, vendors, clients, law enforcement? Depending on which survey you read, anywhere from 30 to 70% of security incidents are from an inside source. Telling your coworker might be tipping off the person responsible for the incident, prompting him to cover his tracks. Overcommunication can result in administrators' interfering with each other while trying to track down the source of the problem — and the more people that know, the greater the risk of bad press. Many state and federal laws now govern the handling of

customer and employee information, and if certain kinds of information are compromised, your legal team will need to be in the loop. An incident handling guide dictates who should know about what kind of incident, facilitating efficient and controlled communication in the first critical hours.

- *I think we have a major virus outbreak.* Should I go through the CEO's inbox and delete suspicious messages? Although manually removing suspicious messages from user mailboxes is a last resort, it is sometimes necessary. However, privacy and security concerns might make this approach inappropriate in some organizations. No system administrator should have to guess at how he should approach privacy issues, and no corporate leader wants to worry about whether her sensitive email is private. A good incident handling guide lets everyone in the organization know how IT staff will handle such information during a security incident.

An incident handling guide gives prepared answers to questions like these based on a collaboration of stakeholders, including system administrators, network engineers, management, legal, and public relations staff. No network engineer should have to weigh the pros and cons of unplugging a Web server in real time. When a staff member follows instructions in the IHG, she knows that she has the full support of management, even if the incident turns out to be a false alarm.

## Key incident handling guide components

An incident handling guide goes well beyond the decisions that need to be made when a problem is first discovered. It provides a framework for making decisions about how best to restore compromised services, whether to contact the authorities, and how to prevent similar incidents (see Figure 1).

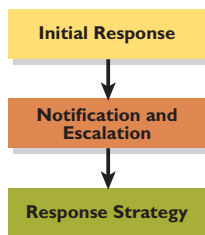


Figure 1: Three key steps in incident handling

### Initial Response

We've all seen enough lawyer-action shows to know that the first thing to do when a crime is discovered is to secure the scene to protect the evidence. The same principle holds true for computer

security incidents. The moment that an incident has been detected, the IHG should guide the process of verifying the event, protecting the evidence, and preventing further damage.

The results of some incidents are obvious, such as a Web-site defacement. The indication of other incidents can be extremely subtle, and the evidence may turn up weeks or months after the incident actually took place. This means that, despite the excitement of discovering a possible incident, there is no excuse not to meticulously follow the IHG's direction to log every action that is performed on the evidence, and to establish a secure, documented chain of custody.

Proper forensics protect an organization by giving it a choice on how to handle the situation. Whether the choice is to handle an incident internally, to bring in a security vendor for proper forensic evidence collection and analysis, or to notify the authorities, having proper evidence allows a company to escalate as needed without fear that the evidence won't hold up in court.

## Notification Protocol

A good incident handling guide has a well-defined communication and escalation protocol for each type of event. An appropriate response to an employee's improper use of equipment might be to notify the human resources department. Often the best response to a forced break-in is to call the police first, and the IT director second.

The guide's notification protocol manages the flow of information so that the right stakeholders are involved at the right time. In general, it's a good idea to funnel information to outside parties through a limited number of points of contact. For example, a system administrator might handle all interactions with a security vendor, while any interaction with the press might be through the public relations department.

## Response Strategy

The incident has been verified, evidence has been secured, and the notification protocol has been put into action. Now the incident handling guide acts as a manual for how to respond to different kinds of incidents, from assessing the damage and neutralizing the threat, to restoring services and making sure that the problem won't recur.

After a physical intrusion, for example, IT staff needs to inventory the compromised space to determine whether assets such as computers, hard drives, or other equipment were stolen. If equipment was stolen, might critical data fall into the wrong hands? A physical break-in might be the first sign that points to a computer intrusion. Was a workstation, server, or network accessed while the intruder had access to the facility? Now the IHG

focuses the response team on the forensic aspects of determining what actions the intruder took while on the premises.

An IHG helps move the organization beyond the incident, directing how to restore services, prevent the breach from happening again, and decide whether outside organizations should be contacted. If you have a worm or virus, chances are that your antivirus vendor has a solution and you can repair the damage internally. But if you detect an intrusion that is directed against specific company data, it might be time to call a security incident specialist or law enforcement.

## Offline Resources

The incident handling guide should be part of an incident handling kit that is ready to go in the event that it's needed. These resources should be in hard copy, so that they can be used even if the systems on which they're stored can't be accessed.

An incident handling kit should include the IHG, network and server configuration information, and an incident handling ledger to record the steps taken after the problem was detected. It might contain tools for unobtrusively capturing the contents of system disks, evidence logs to document the chain of custody, and tamper-proof seals and bags to secure evidence such as hard drives, printouts, and captured data. If your staff isn't trained in computer forensics, your incident handling guide should include directions on when to call in the experts.

## Building your own incident handling guide

Every organization is different, and so is every incident handling guide. Pulling the network connection from a Web server might be a perfectly appropriate response to an intrusion at one company, and exactly the wrong thing at another. Because there is no golden incident handling plan that every company can follow, it's important to work through the answers to critical response questions with all of the appropriate stakeholders involved. This means that your incident handling guide can't be written in the CTO's office. The process should involve buy-in from the CEO, managers, network engineers, system administrators, legal staff, human resources, public relations, and building security services.

Regardless of the size of your organization, your incident handling guide is a key asset for securing your systems and networks. Without a clear understanding of the steps to follow in response to an incident, your response will be muddy guesswork at best. If you have a plan, take the time to review it and perform a drill. If you don't have one, create one. Make sure that your computer security situation isn't like a building without clearly marked fire exits. ■

*This article was reprinted from the Q1 2006 issue of The Barking Seal, a publication of Applied Trust. You can subscribe to The Barking Seal online at <http://www.appliedtrust.com/barkingseal>. "Applied Trust" and the "Seal on a Rock" Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.*