Incident Response & Forensic Analysis

At a Glance, HALOCK Security Labs provides comprehensive and discreet incident response and forensic analysis. Our examiners are experienced with handling intrusions, criminal investigations and sensitive internal matters. Involving HALOCK early in the situation can help you decide what type of response is best for your situation.

Our Certified Forensic Analysts can assist in compromise events such as security breaches, unexplained system failures, policy violations, information leaks, fraud, electronic threats, Web site defacement, monitoring alerts and other suspicious activity that can be traced electronically.

We know when and how to work with law enforcement, we understand the needs of your legal counsel and we can help protect your interests and minimize liabilities.

Emergency Response

800-925-0559

A compromise event is typically a very busy "**All Hands On Deck**" time with system administrators, application experts, engineers, users and management all scrambling to get the affected resources back in operation and determine the extent of the damage.

These events, however, must be approached with **caution** as the improper handling of computer systems immediately following a catastrophic event is the leading causes of **data loss**.

One data point to keep in mind is that the total average cost of a data breach was **$197 per compromised record** in 2007, up from $182 in 2006, and from $138 in 2005.

Pricing for HALOCK's Forensic Analysis and eDiscovery experts is time and materials-based and begins at $300 per hour.

Typical hard-drive acquisition rates begin at $500 and hard-drive analysis begins at $1000 per drive. We can also provide expert court testimony at $450 per hour.

HALOCKSecurityLabs

www.halock.com | 1.866.781.7799

Solution Details

The Method

When a 'compromise event' causes chaos in your team, our team calmly follows this incident response methodology

Response

In a crisis, rely on HALOCK for these important services

- Emergency phone consulting
- Forensic strategy consulting
- First responder training
- Live incident response
- Forensic examination
- Legal testimony
- eDiscovery examination

Phase 1 - Preparation and Training

- Establish baseline security levels
- Assign roles and responsibilities
- Train personnel
- Perform day-to-day monitoring

Phase 2 - Identification

- Suspected incident detected
- IRT (Incident Response Team)
- First responder assessment
- Determine type of threat(s)
- Determine affected resources
- Eliminate false positives

Phase 3 - Containment

- Monitor and/or stop hostile activity
- Isolate affected resource(s)
- Ensure integrity of data
- Ensure availability of critical services

Phase 4 - Eradication

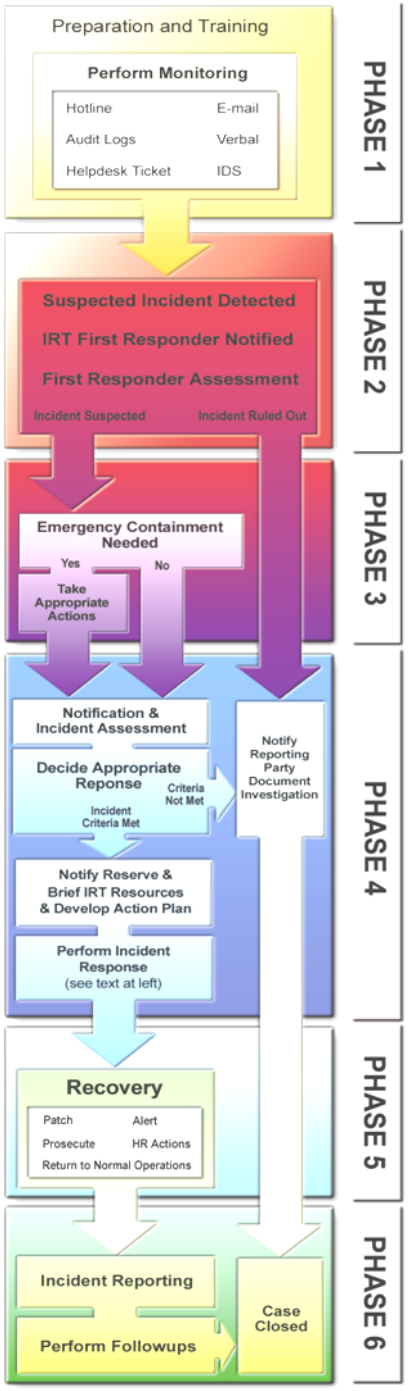
- Incident response (IR) manager notified
- IR manager assessment
- Decide appropriate response
- Notify reserve & brief IRT resources
- Perform Incident Response

Phase 5 - Recovery

- Patch
- Alert
- Prosecute
- HR actions
- Return to normal operations

Phase 6 - Report & Follow-up

- Document incident information and brief
- Document lessons learned
- Improve policies, guidelines and procedures
- Improve infrastructure as warranted



HALOCKSecurityLabs

www.halock.com | 1.866.781.7799