

INCIDENT RESPONSE

No security system is perfect, and cyber attackers can wreak havoc on an organization if unchecked; consequently, swift and decisive action is necessary to contain the damage, determine the exposure, mitigate the risk, and protect against future events.

OnlineSecurity's Incident Response Team (IRT) provides organizations with investigative, risk mitigation, and crisis management expertise in the critical 24 to 72 hours after a cyber security breach.

Service Description

- ▶ OnlineSecurity has a 24 hour hotline, 310.245.2903, to coordinate incident response. Clients calling the hotline will obtain immediate advice on damage control and risk mitigation.

Incident response can involve a wide range of security incidents including, but not limited to:

- Hacking, cyber trespass, webpage hijacking, denial of service attacks, email spoofing
- Social engineering attacks, internal fraud and abuse
- ▶ Depending on the nature of the incident a variety of techniques may be used including but not limited to:
 - Log file review and analysis, computer and network forensics, IP & email tracing
 - Online surveillance, honeypot networks, passive and active intelligence, packet capture and analysis

Delivery Mechanism

- ▶ The IRT can respond anywhere in the US within 24 hours and typically will be on site within 3 to 6 hours.
- ▶ The initial phase of the incident response will occur at the client site as information is analyzed and evidence is collected. The majority of the subsequent investigative work will be done from OnlineSecurity investigative headquarters.
- ▶ Throughout the investigative process, OnlineSecurity's investigators will follow court accepted investigative and evidence handling protocols, so that in the event the evidence must be presented in court, OnlineSecurity can testify to the authenticity, integrity, and veracity of the evidence.

Deliverables

- ▶ OnlineSecurity will provide to the client a detailed incident report encompassing the details (who, what, and how) of the incident, technical analysis, evidence collected, and investigative analysis.

Pricing

- ▶ Incident Response pricing starts at \$225/hour with a minimum of eight hours.
- ▶ Quotes for incident response will be based on the specific scope of the work and will be priced based on the estimated time and material required.
- ▶ Storage and evidence handling for twelve calendar months will be included in the base cost of all quotes, and additional storage and handling (beyond the first year) will be billed based on the amount of evidence.
- ▶ Expenses are billed on a 'no- load' pass through basis, and travel time is billed at 1/2 rate.

Expert witness testimony is an additional service beyond the scope of IT investigations and will be billed separately.

For more information contact OnlineLabs at 310.815.8855 x212 or info@onlinelabs.com

L

Los Angeles

5870 W. Jefferson Blvd., Suite A
Los Angeles, CA 90016
voice: 310.815.8855
fax: 310.815.8808

New York

Boston

Seattle