Incident Management Services

PREPARING FOR THE INEVITABLE COMPROMISE

Identify. Respond. Contain. Remediate.

These days it's not asking if — it's judging when. When will your system experience a threat? When will your client information be exposed to an attack? When will a breach cripple your organization and cost you your reputation, time, and money?

The financial impact of data compromise is growing, based on the results of Ponemon Institute research. With an increase of 15 percent in 2013 over 2012, an expected rise again in 2014, and an estimated average financial impact of $3.5 million U.S. dollars for each identified breach, the toll on businesses could be catastrophic.

Are you prepared? Does your in-house team have the knowledge, the resources — and the bandwidth — to address situations like these on its own? If you use Foresite, you don't need to answer these questions.

Rapid Response. Peace of Mind.

Foresite's Incident Management specializes in rapid response protocols that contain and remediate imminent threats and minimize impacts on your organization. In the midst of a crisis, we react immediately.

Even better: We can be proactive in identifying compromises before the crisis becomes full-blown. Based on the Ponemon Institute report, the average time to contain an incident was 31 days with an average cost of more than $600,000. Identifying a compromise shortens its days to containment and lowers its cost.

FORESITE ALWAYS BEATS HINDSIGHT

PROACTIVE SERVICES

Breach Identification Services include:

- Collection of endpoint, server memory, and configuration information to identify malicious or unknown behavior

Incident Management Policy & Process Development and Testing Services include:

- Review of policies, processes, and skills to assess levels of strengths and weaknesses within an organization

REACTIVE SERVICES

Digital Forensic Services include:

- Evidence collection of drives and memory devices
- Drive duplication
- Processing and analysis of drives and memory

For scenarios that include:

- Drive collection and preservation
- Malware infection
- Sensitive data ex-filtration
- Inappropriate usage

Incident Response

- Available ad hoc or upon retainer

Understanding the situation.

We begin by gathering information about what is occurring, how it was identified, its impact on the organization, and any response processes initiated by our clients.

Identifying client goals.

We work directly with our clients to identify aggressive but reachable goals surrounding the identified incident.

Collecting pertinent evidence.

We collect device information (i.e. memory disk), logs, and network packets to identify the extent of an incident. This collection process is strategic and targets only pertinent information and devices, allowing for more efficient analysis and faster results.

Performing analysis.

We develop a detailed picture of the incident by investigating all aspects of the collected evidence in the context of the overall situation and our client's goals.

Defining results-based direction.

At this stage, we apply all known information towards defining a direction for the investigation based on known facts and likely impact. We communicate this information to our client contacts and responders to enable them to make a well-informed and effective business decision for their organization.

Developing remediation and deployment strategies.

We gauge the size and complexity of the level of effort required to fix the problem. Moreover, we evaluate the ability of our clients to perform tasks that address the type and extent of the incident and to secure their environment. As part of this process, Foresite delivers a comprehensive plan and assists with implementation.

RETAIN FORESITE FOR IMMEDIATE RESPONSE AND PEACE OF MIND

Standard Retainer includes:

- 40 hours or more of services (Discounts available)
- Escalation path through Foresite Security Operations Center (SOC)
- 48-hour Service Level Agreement, U.S.-based engagement, for arrival of onsite consultants

Premier Retainer includes:

- 80 hours or more of services (Discounts available)
- Escalation path through primary incident handlers
- 24-hour Service Level Agreement, U.S.-based engagement, for arrival of onsite consultants

Producing the investigation report.

We deliver to our clients a final report that documents the steps taken and actions performed from the onset of the engagement through the completion of remediation efforts. We organize the report into sections that address the different audiences that will be reviewing the results: upper management, technical staff, and third-party organizations.

Providing continued post-incident support and follow-up.

We maintain frequent contact with our clients to determine whether any additional events have been identified, to confirm the completion of recommendations, and to address any questions and/or concerns from the client.