IR Summit Strategy Panel

Rocktober 13, 2008

What Type of Data Loss Should We Be More Concerned With, PII or PCI?

Data Loss Impact Analysis

- Decide What Data Loss Will Have the Greatest Business Impact
  - PCI
  - PII
  - IP
  - Trade Secrets
  - Financial Documents

MANDIANT
INTELLIGENT INFORMATION SECURITY

3

What Should Be Your First Priority, Detailed Descriptions of the Data Stolen, or Detailed Descriptions of How the Break-In Occurred?

MANDIANT®
INTELLIGENT INFORMATION SECURITY

Answer: Aim for Both, but Prioritize

- Priority 1a – Disarm The Attacker
- Priority 1b – Comprehend Potential Data Loss

MANDIANT
INTELLIGENT INFORMATION SECURITY

5

Realities

- Stop the Bleeding Before Diagnosing How Many Bones are Broken
- Its Too Late to Do Damage Assessment at the End of the Incident
- Data Loss is Almost Always an Opinion

MANDIANT
INTELLIGENT INFORMATION SECURITY

6

Three Questions to Ask Outside Firms When Seeking Assistance

The Interview

- When can you get here?
- What are the master services agreement terms (includes NDA, who the contract is with, non-compete, non-solicitation)?
- What experience/references do you have?

The Interview

- What is are the financial terms: rate, expenses, invoicing, timing, etc?
- What investigative steps would you normally take in a situation like this?
- How will you communicate with us?
- What expectations should we have about how long this will take?
- What can we reasonably expect to accomplish: stop incident, secure environment, determine exposure, ID bad-guy, etc?
- What should I do or not do between now and when your team arrives onsite?
- How large would your team be and what roles would they have/play?

MANDIANT
INTELLIGENT INFORMATION SECURITY

9

Interpretation of Your Response

- CEO/Executives
  - Commitment Assessment
- Management
  - Ability to Get Things Done
  - Incident Response Comprehension
  - Trust in Third Party Assistance
- Technicians
  - Technical Prowess
  - Network's Ability To Detect, Collect and Remediate
  - Willingness to Accept Assistance

MANDIANT
INTELLIGENT INFORMATION SECURITY

10

What Are The Top 3 Incident Response/Forensic Mistakes That Organizations Routinely Make?

Top Challenges

- Virtually All Challenges Derive from:
  - Failure to Document Appropriately
  - Failure to Assign Incident Ownership

Failure to Document Appropriately

MANDIANT®
INTELLIGENT INFORMATION SECURITY

Understand Your Audiences

- CEO/Executive Leadership
- Legal / Compliance
- Technical
- Insurance

Management Concerns (Board and CEO)

- What is the Incident's Impact on Business?
- Do We have to Notify our Clients?
- Do We have to Notify our Stock Holders?
- What are other DoD Contractors Doing about this Sort of Thing?

MANDIANT
INTELLIGENT INFORMATION SECURITY

15

Legal Counsel Concerns

- What are the applicable regulations or statutes that impact our organization's response to the security breach?
- Which state laws are applicable? Which might be in the future?
- Are there any contractual obligations that impact our incident response strategy?

MANDIANT
INTELLIGENT INFORMATION SECURITY

16

Legal Counsel Concerns

- How might public knowledge of the compromise impact the organization?
- Does notifying our customers increase the likelihood of a lawsuit?

MANDIANT
INTELLIGENT INFORMATION SECURITY

17

Technical Management (CIO)

- How long were we exposed?
- How many systems have we inspected?
  - #
  - Name - IP
  - Indicator / Priority
  - Status
- How many systems are compromised?
- What data, if any, was compromised (i.e., viewed, downloaded, or copied)?
  - Export control data?
  - PII

MANDIANT
INTELLIGENT INFORMATION SECURITY

18

Technical Management (CIO)

- What was the Attack Vector?
- What countermeasures are we taking?
- What are the chances that our countermeasures will succeed?
- Is the incident ongoing? Preventable?
- Is there a risk of insider involvement?

MANDIANT
INTELLIGENT INFORMATION SECURITY

19

Establish Controls Early for Knowledge Transfer

- Establish Formal Reporting
  - Forensic Methodologies
  - Forensic Reports
  - Classification and Prioritization of Indicators.
  - Malware Analysis Reports
  - Remediation Step Tracking
- Establish Repository for Reports

MANDIANT
INTELLIGENT INFORMATION SECURITY

20

Failure to Assign Incident Ownership

Challenges: Incident Ownership

- Failure to Assign an Incident Owner often Leads to:
  - Uncertain Dedication of Resources
    - Money
    - Manpower
  - Roles and Responsibilities May Not Be Clearly Defined
  - Uncertain Response Posture (Moderate or Aggressive?).
  - Ambiguous Communication Lines Across Separate Lines of Business.
  - Splinter Cells of Responders.


Questions?
MANDIANT
INTELLIGENT INFORMATION SECURITY
23