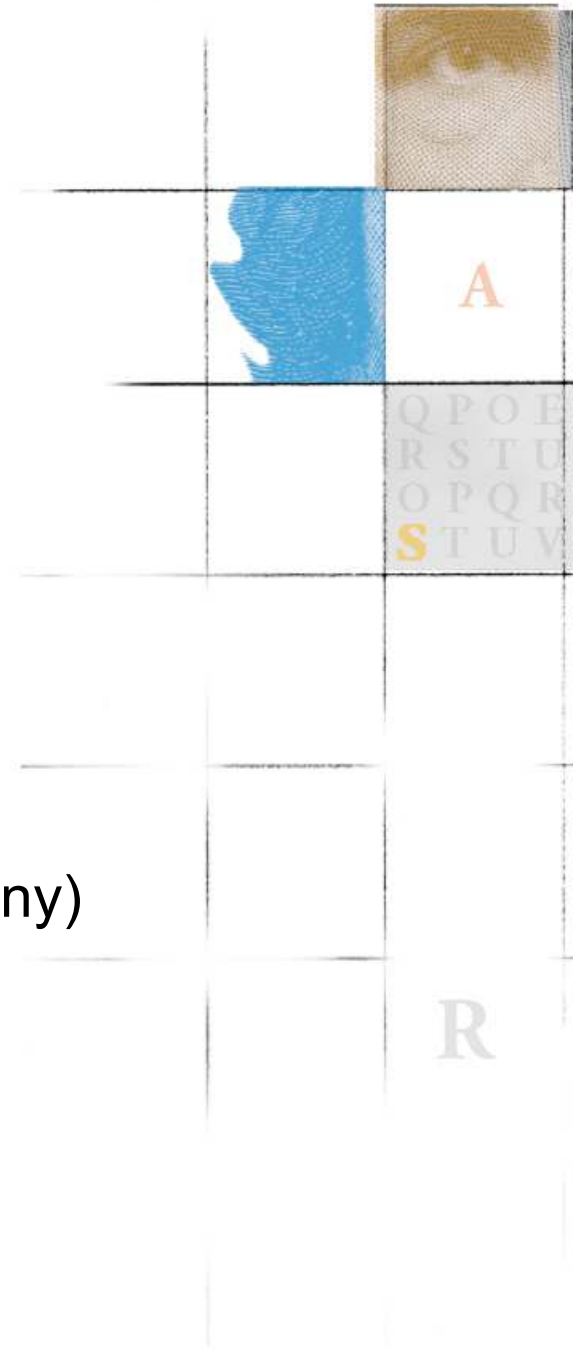
RSA CONFERENCE 2009

How to Prepare for the Five Most Common Security Investigations

Moderator: Evan Wheeler
Omgeo (A DTCC | Thomson Reuters Company)
04/22/09 | Session ID: ESS-202



Panelists

- Jim DeLorimier
  - NJ Manufacturer's Insurance
  - CIRT / Forensic Team Leader
- David Thomas
  - Attorney
  - Greenberg Traurig, LLP
- Lenny Zeltser
  - Security Consulting Manager
  - SAVVIS, Inc.
- Eric Gentry
  - Principal Consultant
  - Verizon Business, Investigative Response Practice

Key Topics

- Mobile Device Loss / Theft
- Malware Infections
- Data Leakage
- Inappropriate Browsing Activity
- Web Server Attacks

Apply @ Work

This panel recommends that the following actions to be applied when you return to work:

- Include notifying law enforcement or regulators, and releasing public breach notifications in table-top scenarios with management
- Verify NDA and/or Confidentiality Agreements are in place and systems are properly bannered
- Make a list of data sources that should be reviewed in advance of an incident (ex. proxy or DNS logs)
- Create playbooks, checklists, procedures, forms, and keyword lists for the 5 categories of investigation
- Test imaging of large drives across your WAN and identify appropriate storage for large evidence files