WEIS 2008
Workshop on the
Economics of
Information Security

Cybercrime Panel – Investigating and Prosecuting Cybercrime

Kathryn Warma, Assistant U.S. Attorney, Washington
Jim Burrell, Assistant Special Agent in Charge, Boston, FBI
Lucy H. Carrillo, Assistant Attorney General, New Hampshire Criminal Justice Bureau
William Cantwell, New Hampshire State Police
Eric Goetz, I3P (moderator)

This panel brings together state and federal law enforcement officials to discuss cybercrime investigations and the challenges posed by prosecuting these offenses. The panel will present a variety of unique perspectives all the way through the law enforcement chain from collecting evidence to convicting cyber criminals. The panel will analyze emerging cybercrime trends in an environment where cyber attacks are increasingly perpetrated by professional criminals with a profit motive. Panelists will discuss how cybercrime cases actually unfold, how law enforcement officials interface with industry and other federal, state and local agencies, and how they navigate the maze of jurisdictions. The panel will discuss the following questions:

- Who has jurisdiction over what in cybercrime investigations? How do jurisdictional problems impede investigations? How does law enforcement overcome these challenges in practice?
- How do local, state and federal agencies work together on cybercrime investigations? How and when do they start working with prosecutors to build a case?
- How does it affect jurisdiction if attacks on U.S. systems are routed through machines in other countries?
- What special challenges do cybercrimes pose for law enforcement officials and prosecutors compared to 'conventional' crimes? Does this require specialized knowledge and skills?
- Are companies regularly reporting cybercrime activities and attacks? If not, why are they reluctant?
- Are companies developing capabilities/structures to coordinate with law enforcement on cybercrime investigations? Who at a firm do law enforcement officials interface with?
- How are companies preparing for cyber attacks?
- Are you seeing changing trends in cybercrime (i.e., professionalization of cybercrime activities)? What are the latest schemes you are seeing?
- How are cyber criminals utilizing the latest technologies? Is this changing the nature of cybercrime and posing new challenges for law enforcement (e.g., how to deal with crimes in virtual worlds)?
- From your experience how would you articulate the business case for the cybercriminal? What can be done do to ensure that cybercrime does not pay? Which parameters can we change so that the cybercrime equation is less appealing?