FCC Cyber Security Workshop
Panel 2: Detect and Respond

Dale Drew, Global Security

Level 3 Communications, LLC

Detection: The Tools

- Monitoring for trends and techniques
  - Industry and government forums
  - Grey and Blackhat forums
  - Netflow & SFlow– Core and Edge

- Real time detection of events
  - Netflow & SFlow – better sampling capability needed
  - DPI - Swarming
  - Element log files
  - Registration data
  - Physical Security integration
  - Etc

Detection: The Tools

- People
  - Skilled and trained personnel are key!
  - Regular incident testing
  - Continuous training
- Attacks are becoming much more social in nature
  - Go after the infrastructure by attacking the people who operate it

Detect and Respond: Commercial

- Plenty of formal and informal avenues exist to share information
  - Who to include/exclude often becomes the problem
  - ISP Threat sharing forums
  - Vendor coordination – although becoming more difficult

- On the topic of vendors
  - Edge vendors are becoming more versatile, more capable in detecting/stoping attacks
  - Core vendors care about speed

Detect and Respond: Government

- Plenty of formal and informal avenues exist to share information
  - Circle of trust is easier here
  - MANY forums to choose from
  - Information sharing needs to be more bi-directional

ISP Needs

- Vendors to be more accountable for security of their products
- Better capable DPI systems
- Better Netflow monitoring capabilities
- More information sharing between forums and from the Government
- More focus on the Layer 8 (end user) problem; social networking attacks
  - Captcha + passwords?

THANK YOU!