Cybersecurity: The Impact Of Broadband Technology

Federal Communications Commission
Public Safety Workshop
www.broadband.gov

August 25, 2009

Marcus H. Sachs, P.E.
Verizon

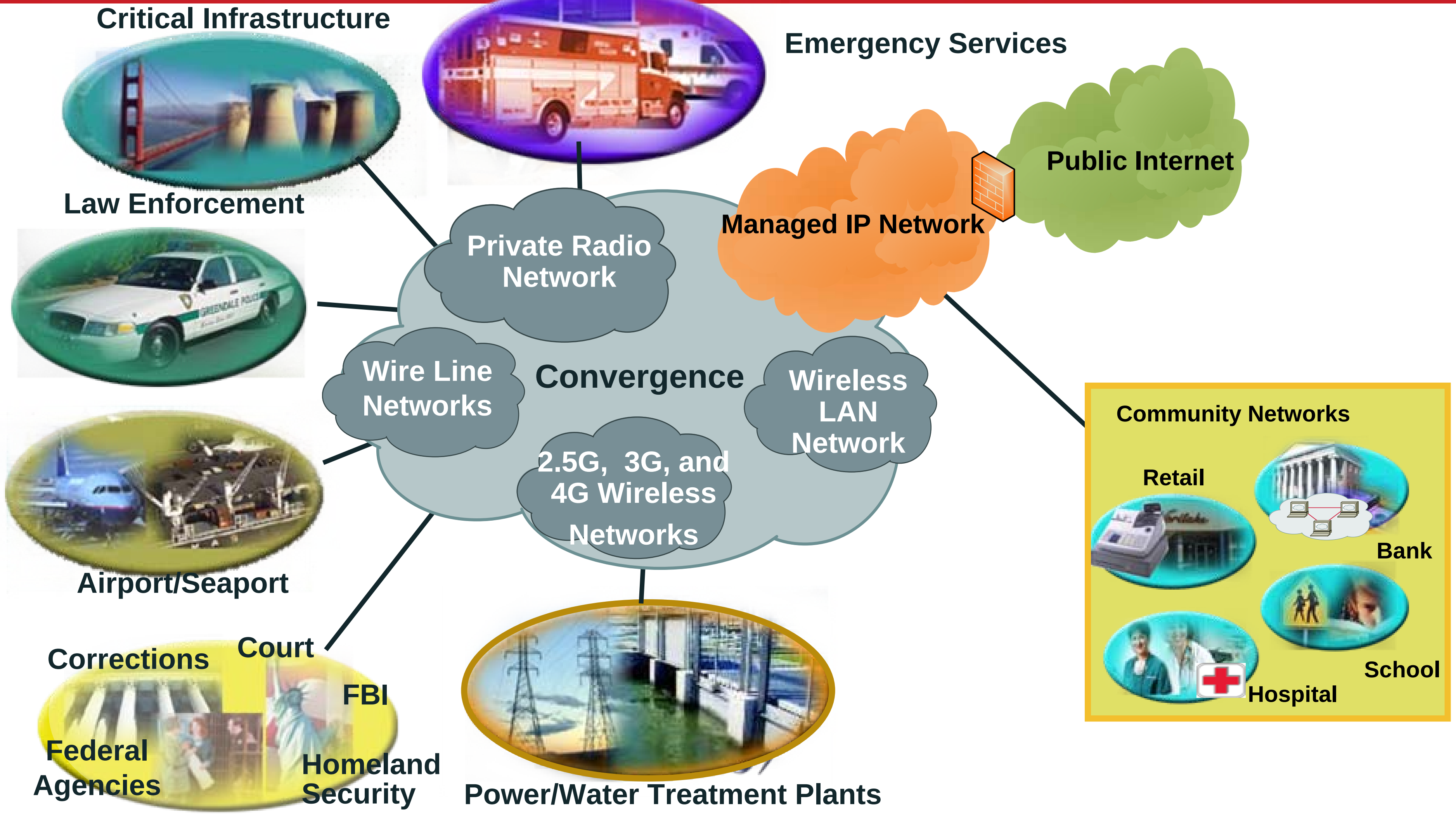
Overview of Online Security Risks

- **Internet Fraud**
  - Website spoofing
  - Link and DNS manipulation
  - Spam
- **Infections and Malware**
  - Viruses
  - Worms
- **Malicious Payloads**
  - Spyware
  - Bots
  - Keystroke Loggers
  - Dialers
- **Concealed Intrusions**
  - Trojan horses
  - Root kits
  - Backdoors
- **Malware Objectives**
  - Forced advertising
  - Distributing spam
  - Launching Distributed Denial-of-Service attacks
  - Stealing personal data like social security numbers

Emerging Threats

- Leveraging social networks and viral applications to quickly establish botnets
- Targeting smart phones and other open devices that communicate over high-speed wireless networks
- Hijacking VOIP systems for identity fraud, toll fraud, or theft of sensitive information
- Cyber warfare targeted at the U.S. economy and infrastructure

Protecting Networks and Customers



Keeping The Network Safe – Industry Responsibilities

- Identify and mitigate spam, viruses and other malware
- Analyze and help mitigate security breaches
- Conduct security audits for enterprise and government customers
- Provide testing and certification for security products and network connected devices
- Offer parental controls and security products

Smart Networks Could Improve Online Security and Openness

- Identifying and intelligently mitigating malicious activity
- Prioritizing communications in support of first responders and public safety officials
- Increasing the open and competitive nature of global data networks by removing or mitigating threats and weaknesses
- Enabling new and innovative applications for the smart grid and Health IT

Next Steps