AT&T Cybersecurity Overview for NARUC

Chris Boyer – AVP – Global Public Policy

July 13, 2015

AT&T approach to network security

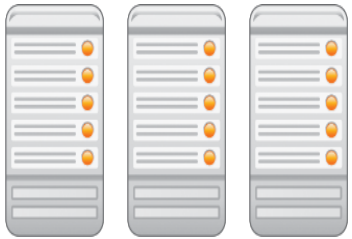
- **24x7 global situational awareness**
  Near real-time analysis of security indicators
- **Operate largest IP/MPLS Core Infrastructure**
  Real time global situational awareness
  Integrated management and response capability
- **Embed security capabilities in network**
  Security enforcement nodes
  Enterprise protection and managed services
- **Secure core network infrastructure**
  Traffic Separation, hide core infrastructure, hardening, filtering/monitoring traffic flows

Providing value-deep visibility, analytics, and response

Extensive data collection

- Over 90 Petabytes of data traffic passes through the AT&T Network on an average business day

Robust security analytics



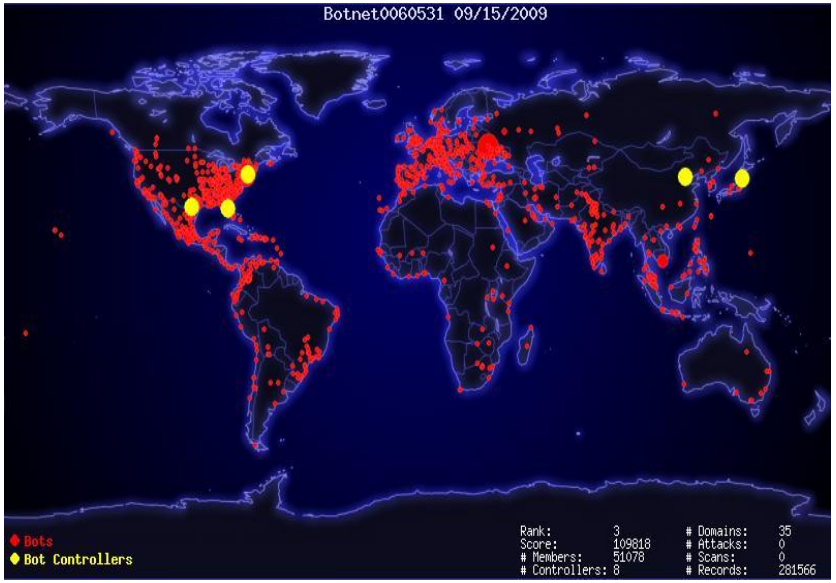
- Hundreds of millions of events reduced to hundreds of actionable alerts daily

Expert threat response & mitigation

- 24x7 redundant Security Operations Centers
- Approximately 2000 security experts

Identifying the anomalies

AT&T global security nodes, botnet illustration



Evolution of threat management

Traditional approach

- Monitor traffic in and out of perimeter
- Compare against known signatures
- Generate alerts to SOC for investigation

The traditional approach is changing

- What's the perimeter?
- Threats evolving at increasing rate
- Overwhelming amounts of data from many sources across complex environments

Effective threat management must…

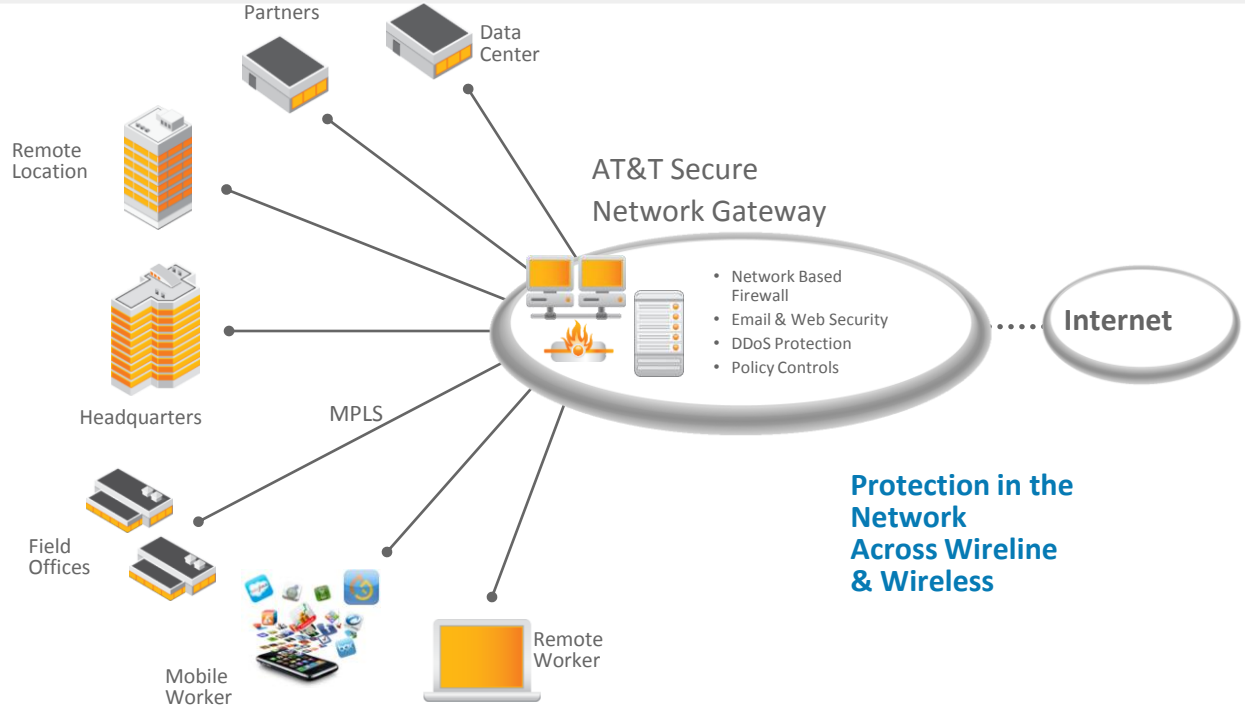
- Collect and aggregate data from multiple sources
- Turn data into information
- Respond real-time with changes to policies and filtering

Perimeter security?

70% of threats go undetected
by anti-virus software

29% work from multiple locations,
using multiple devices and apps

Evolution to Simple, Efficient Network Environment



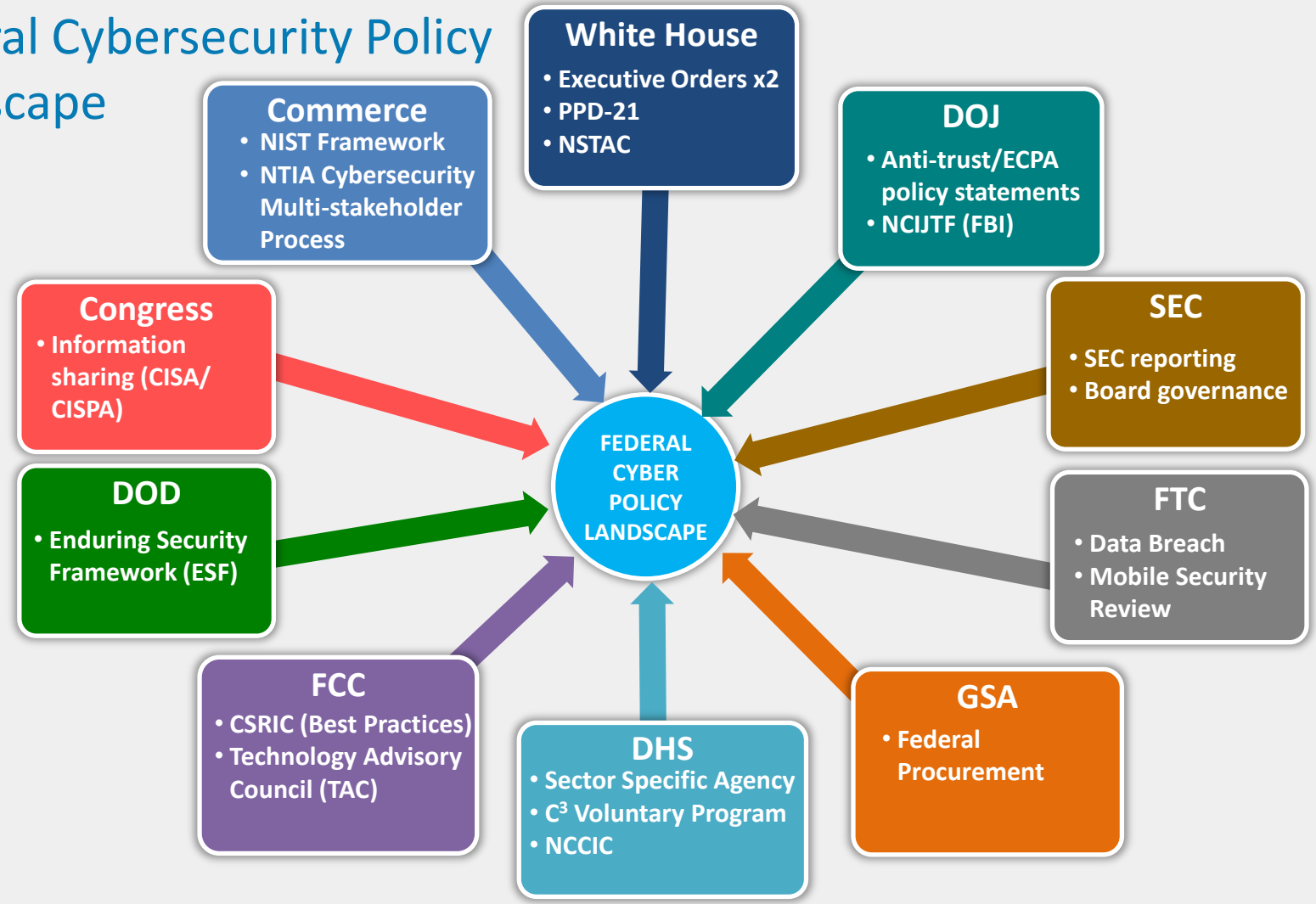
Protection in the Network Across Wireline & Wireless

Public private partnerships are the foundation for pubic policy addressing for cybersecurity

"Public-private partnerships have fostered information sharing and served as a foundation for U.S. critical infrastructure protection and cybersecurity policy for over a decade. During that time, the Federal government and the private sector have engaged in a number of forums on cybersecurity and information and communications infrastructure issues."

- The White House Cyberspace Policy Review

Federal Cybersecurity Policy Landscape



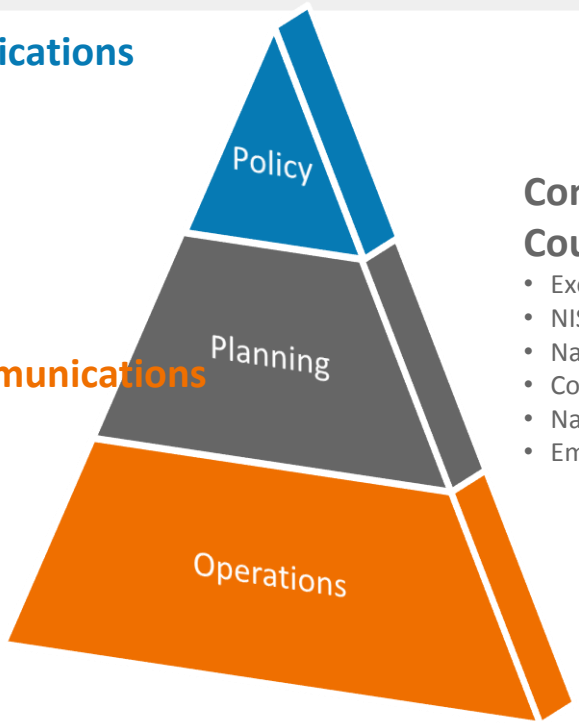
Communications sector partnership w/ government

National Security Telecommunications Advisory Committee (NSTAC)

- White House 60 Day Review
- Cloud Security s
- Promoted NCCIC, NSTIC etc.

National Cybersecurity & Communications Integration Center (NCCIC)

- On call 24/7 center
- US CERT
- ICS CERT
- National Coordinating Center (NCC)



Communications Sector Coordinating Council (CSCC)

- Executive Order Implementation
- NIST Framework
- National Sector Risk Assessment (NSRA)
- Communications Sector Specific Plan (CSSP)
- National Incident Response Plan
- Emerging Security Framework (ESF)

Policy considerations for state governments

- Partner with private sector/Federal agencies to protect critical infrastructure by leveraging work that is being done in being done in various federal, regional, state and local venues (e.g., MS-ISAC; State, Local and Tribal Coordinating Council; National Level Exercise)

- Raise awareness across state/local government and coordinate response in event of a major cyber incident; e.g., eSecure Your eCity in San Diego, Michigan Cybersecurity Program etc.

- Preserve private sector incentives for investment, innovation; and flexibility to respond to threats. There is no one-sized fits all solution to cybersecurity.

- Enhance awareness and education - support the National Cybersecurity Awareness Campaign, STOP THINK CONNECT, build computer security and digital citizenship into classroom curriculum, increase importance of secure software design at University level.

- Increase support for law enforcement in pursuing cyber criminals

- Lead by Example – deploy cyber security solutions across state government systems