TASC

The Era of Outsourcing

Mark Leary

CISO

March 16, 2011

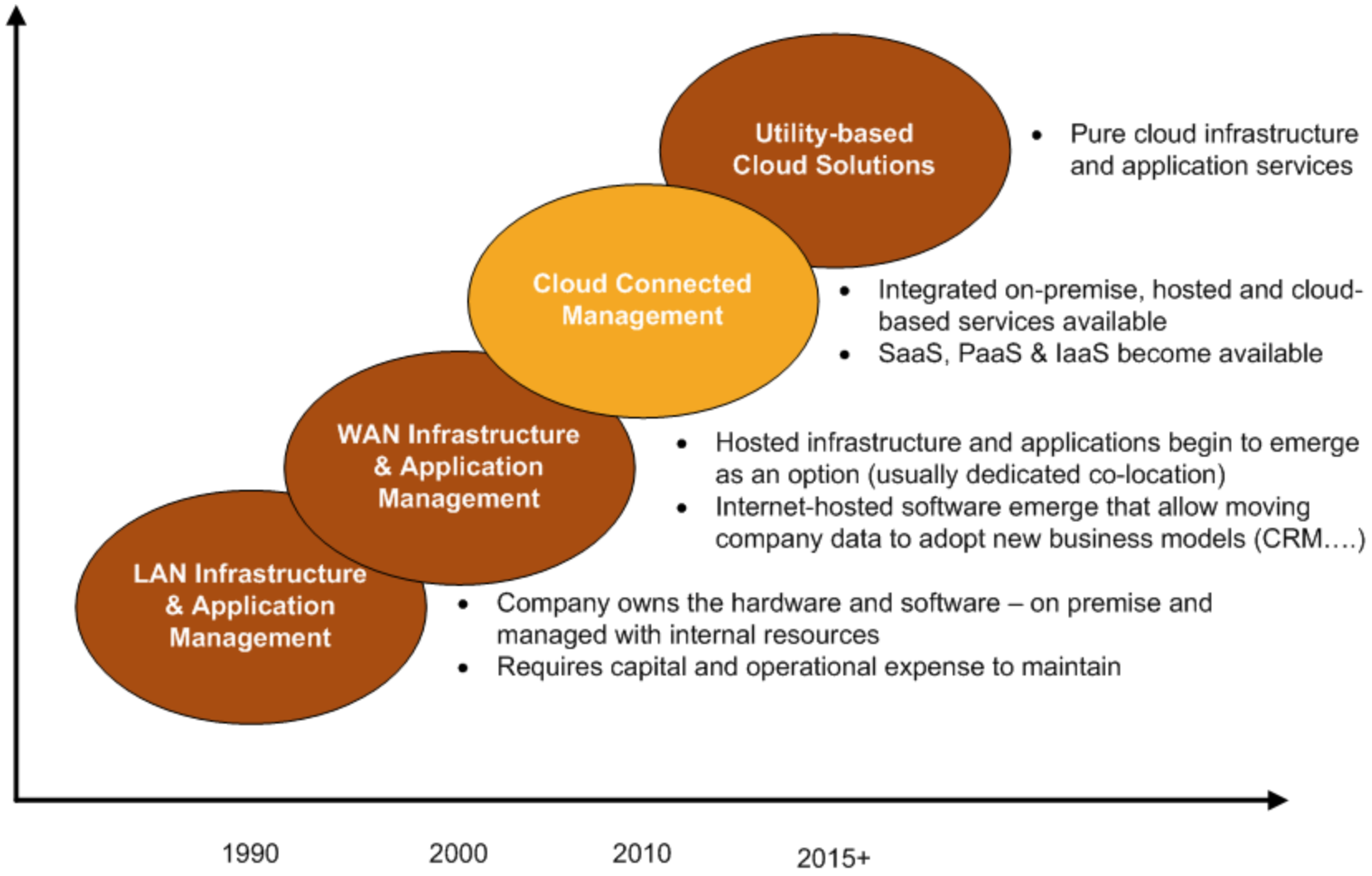
Our Company

- Founded in 1966
- Headquartered in Chantilly, VA
- More than 5,000 employees in 40 locations
- $1.55 billion in annual revenue
- Supports 300+ federal contracts in intelligence, defense, homeland security and aviation

Our Core Capabilities

- Systems engineering and integration
- Program, financial and acquisition management
- Mission operations, analysis and engineering
- System and policy analysis
- Advanced concept and technology development
- Test and evaluation
- Independent verification and validation
- Cybersecurity

IT Outsourcing Evolution



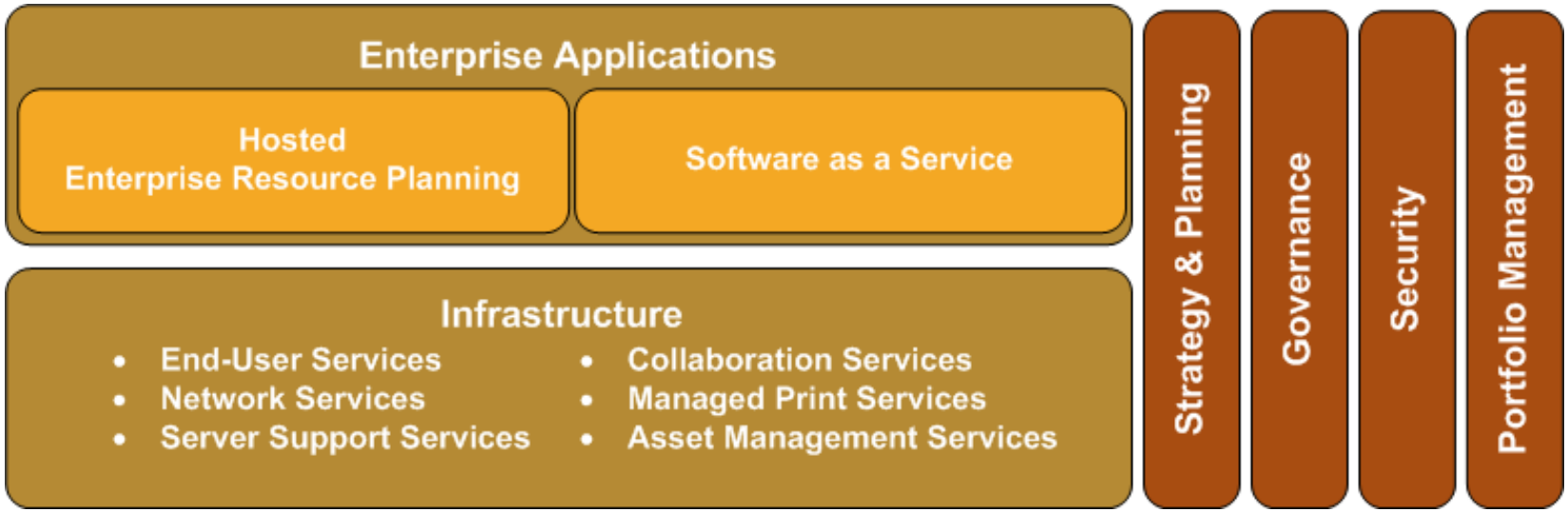
TASC

Security Challenges to Outsourcing

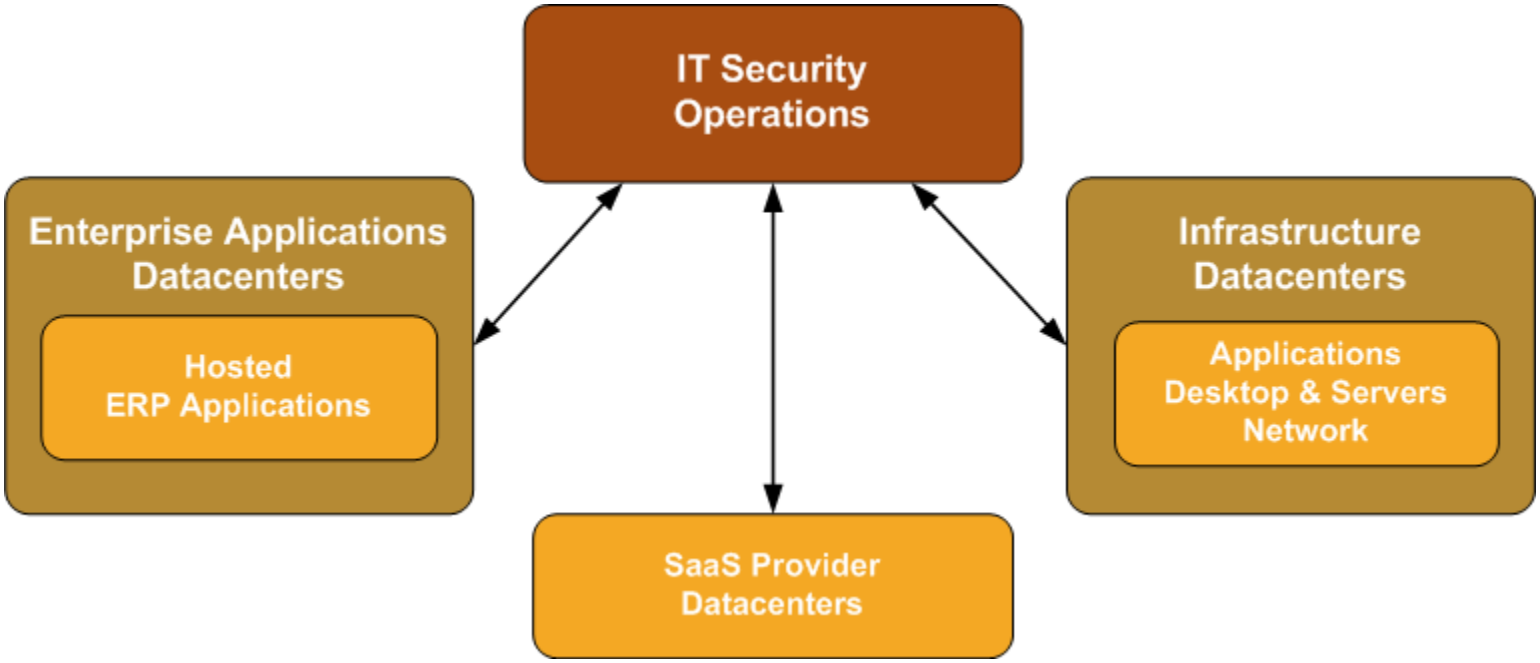
- Regulatory compliance
  - Company is held responsible for the security and integrity of the data
- Privileged Access
  - Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass controls
- Data Segregation
  - Data is typically in a shared environment alongside data from other customers
- Data Location
  - Company may not know exactly where data is hosted
- Disaster Recovery
  - Service provider should outline what will happen to data in case of a disaster
- Investigations & Forensics
  - Investigating inappropriate or illegal activity for a hosted environment is hard…and may be impossible in cloud offerings

Our Outsourcing Model

- Focus On Core Activities
- Service Continuity
- Reduced Overhead
- Cost And Efficiency Savings
- Staffing Flexibility
- Develop Internal Staff



IT Security & Outsourcing



- Information Security Management
- Physical and Personnel Security
- Identity Management
- Endpoint and Server Security
- Gateway and Network Security
- Web and Application Security

For Your Consideration

- Provide contract clauses that address security in a manner consistent with company policies
  - Inform and enforce company policies and standards with the provider
- Review technical risks with Procurement when developing security clauses for outsourcing contracts
- Review service provider's audit reports (if available) to ensure that their level of effort addresses data security
- Ensure service providers provide adequate information about architecture, functionality and security to identify risks
- Ensure that security requirements are imposed on SaaS providers (might not be possible…)
  - Use a security checklist as a starting point
- Ensure infrastructure and application services can support potential eDiscovery and investigation needs
- Use third-party vulnerability assessment firms to validate provider's security