Protecting Citizen Information and The Public Trust

A Call to Action For State and Local Government

Todd Waskelis
Vice President, AT&T Security Consulting

Kim Bilderback,
Application Sales Director for Security
Discussion Topics

• Security Threat Landscape

• Common Areas of Risk
  o Application Security
  o PCI
  o Mobile Devices

• A Call to Action: Information Risk Management
Inadequate Security – Common, Costly, Risky

According to the Identity Theft Resource Center, the government sector was accountable for nearly 16% of data breaches identified in 2010*

As reported by the 2011 Gov Info Security Online Survey results, where more than 200 IT security professionals working for local, state and federal governments were polled, “One-third concede their agencies fail to do an adequate job to counter threats.”**

According to the Privacy Rights Clearinghouse, over 500 million records have been breached since reporting began in 2005. ***

***Privacy Rights Clearinghouse, Chronology of Data Breaches, [www.privacyrights.org/data-breach#Total](http://www.privacyrights.org/data-breach#Total)
The Macro Environment At-A-Glance

- Budget Constraints & Cost Reductions Not Seen Before
- Pressure to Increase Transparency and Accountability
- Online Access and Delivery of Services – “The Norm”

“State and local governments have shed 397,000 jobs since August 2008, falling to their lowest level since the late 1980s, according to the Center on Budget and Policy Priorities.”
A Challenging Digital Landscape

- Investing in advanced technologies
- Distributed computing environments
- Exponential growth in digital storage requirements
- Legacy systems and near end of life technology
- Evolving Regulatory Requirements
Unrelenting Attacks and Breaches

- Spam, phishing, hacking, and network probes increasing
- Organized crime, geopolitical, Advanced Persistent Threats (APT)
- Malware – Viruses, Worms, Trojans, Spyware
Drivers for Staying Current

Consequences

- Disruption of citizen services including public safety
- Loss of Citizens’ Trust
- Legal compliance requirements and associated financial penalties

Benefits

- Improved transparency and collaboration
- Enhanced productivity and cost efficiency
- Improved delivery of citizen services

Security and Privacy: Top Priorities for State and Local Government

NASCIO 2010 Cyber Security Study

“In the current environment of elevated cyber threats, states are faced with circumstances that have the potential to produce a perfect storm…”

NASCIO Call to Action For New Governors

“As government moves forward in adoption of new technologies to streamline services and meet growing citizen expectations, it is critical that security mechanisms associated with those advancements be fully understood and risks reevaluated.”
The Bottom Line...

- Today’s Networks are Different
- Adversaries are More Sophisticated
- Security Paradigm Shift is Needed
Common Areas of Risk Today

Application security

PCI – Payment Card Industry Standards

Mobile Devices
Application Security

Protecting Public Trust
Today, Software is Everywhere

Users demand their applications anywhere, anytime

On Premise: desktops and servers

On Demand: cloud and hosted

On The Go: laptops and mobile devices
Applications Are the Focus...

The number and costs of breaches continue to rise

- 80% of successful attacks target the application layer (Gartner)
- 60% of applications fail to achieve security requirements on initial testing (State of Application Security from Dark Reading)
- 90% of internally developed applications have at least one issue listed in the Open Web Application Security Project’s (OWASP) Top Ten list or SANS Top 25

* Ponemon Institute, 2008 Annual Study: $U.S. Cost of a Data Breach
^Source: The Open Security Foundation

Total average cost of a data breach per compromised record* $202
Average # of compromised records per breach^ 30,000
Average Total Cost per breach* $6 M
Action Plan for Securing Applications

- **Adopt** a secure software development lifecycle (SDLC)
- **Build** Scalable application security programs
- **Analyze** Application Security Risks
- **Quantify** Application Security Risks
- **Streamline** Security Operations
- **Reduce** Application Code security flaws
- **Propagate** best practices
- **Address** Application Security in contracts
PCI – Payment Card Industry Compliance

Protecting the Citizen’s Credit Card Data
Common Challenges for PCI Compliance

What is the most efficient and effective way to achieve and maintain PCI compliance?

How can we insulate the remediation approach from industry debate?

How do we ensure that our remediation approach will stand the test of time?

What is the best way to be proactive and compliant as soon as possible?
Top Focus Areas for PCI

• Organizational Security
• Mature Software Development
• Product Vulnerability Management
• Secure Implementation
• Emerging Payment Technologies
• Formalize Processes & Procedures
Updates to the Standard: PCI DSS v. 2.0

- Emerging technologies
  - Virtualization
  - Tokenization
  - End-to-end encryption
- EMV standard (chip cards)
- PCI Council guidance for compliance
- Impact on PCI
Emerging Technologies: The Road Ahead

- Encryption, tokenization are still maturing
- Encryption security depends on protecting key
- Review PCI Council Guidance
- Review Card Member Organization Guidance
Action Plan for Adoption of Emerging Technologies in PCI

- Strike the balance between risk and compliance
- Understand data flow for the entire payment environment
- Identify and leverage synergy between PCI and other compliance efforts
- Rationalize payment processes and consolidate payment data and systems
- Continuously monitor and advance payment card protection
Mobile Security
Evolving Security Needs of Mobility

- Managing and limiting access to sensitive information assets
- Securing the sensitive data stored on the device
- Securing lost or stolen devices
- Securing against Malware – Viruses, worms, Trojans, spyware
- Securing against Direct Attack – Attacking device interfaces, browser exploits, etc.
- Securing against Data Communication Interception – Sniffing data as it is transmitted and received
- Securing against Identity Theft – Accessing resources with a user’s identity or credentials
Suggestions for Mobile Security

Needs to be considered from multiple angles, including:

• Access to the device
• Securing content on the device
• Secure and trusted access to organization’s assets
• Breach/Loss/Theft mitigation

When Applied to a Mobile Workforce
GSMA Mobile World Congress

• More than 80% of organizations do not have policies around accessing organization data remotely using mobile devices.
• Some 45% of organizations are accessing sensitive data with mobile devices.
• Only a third of enterprise mobile users polled said they were using secure mobile devices to access or store organization information.
Information Risk Management

Balancing Security, Risk and Budget
Reality Check – The Potential to Produce “A Perfect Storm”

Comprehensive collection of Personal Identifying Information

Growing reliance on technology and the Internet

State and Local Governments must shore up and modernize the defenses to protect this critical information and these mission critical systems
Lessons Learned from Wikileaks

• Ensure that you know exactly what you need to protect

• Know where the information exists

• Limit access and control of the protected information

• Enforce protection using security measures that include:
  – Hardware restrictions (no removable media)
  – Secure Application configuration
  – Data Loss Prevention (DLP) technologies
  – Continuously monitor for signs of breach
Sensitive Information (PII, PHI) leaks are more common than you think

Adapted based on X.805 Model
Information Risk Management: Striking the Balance

Core Benefits

- Protect Public Trust
- Secure Citizen Information
- Enhance Operational Efficiency
Information Risk Management: Are You Managing the Right Risks?

Information Centric
Risk Based
Repeatable

Information as an asset
Value of the asset
Risk Exposure
Risk Appetite
Choose control
Manage Risk
Security – A Risk that Needs to Be Managed

Strike the Balance

Cost of Confidence versus Cost of Breach
Want more information?
Send an email to:

statelocalgov@att.com

www.att.com/govsecurity