Best of Texas – Cyber Security

Patricia Titus, Director Enterprise Security Strategy
October 14, 2008
What happened – how did we get here

• Post 9-11 reactions to security vulnerabilities
• Point solution troubles
• Converged physical and IT infrastructures
• Doing more with less
• DON’T GIVE UP!
Biggest Challenge: Non-integrated Security
Point solution trouble

Firewalls, intrusion detection systems, intrusion prevention systems, behavior detection, intelligent network security, forensics, encryption, data in motion, filtering, monitoring, anti-virus, anti-spam, anti-phishing, compliance, auditing, vulnerability scanning, log analysis, anti-fraud, mobile device security, secure coding, software assurance, patch management............
Converged Physical Security
Our Cyber Dependency

• Today both public and private sector rely on information systems to perform their missions and business function.

• Enterprise systems must be protected from cyber threats to ensure they are available.

• Significant cyber attacks have overwhelmed security professionals
  – Attacks are aggressive and targeted; many are extremely sophisticated
  – Our adversaries are nation states, terrorist groups, hackers, and those with intentions of compromising critical systems
  – Malicious software deployments making it nearly impossible to protect critical systems and information
Cyber Warfare Attacking Your IT Systems

• The weapons of choice —
  – Laptop computers, hand-held devices, cell phones.
  – Sophisticated attack tools and techniques downloadable from the Internet such as botnets, malicious code, spam, phishing and the list goes on
  – World-wide telecommunication networks including telephone networks, radio, and microwave.

Resulting in low-cost, highly destructive attack potential. Not mention if they fail in the hack attempt there’s little knowledge they even tried (unlike a fail suicide bomber).
What’s at stake and who’s the target

• Federal government
• Public sector
• Private sector
• Information systems supporting critical infrastructures (public and private sector) including:
  – Energy (electrical, nuclear, gas and oil, dams)
  – Transportation (air, road, rail, port, waterways)
  – Public Health Systems / Emergency Services
  – Information and Telecommunications
  – Defense Industry
  – Banking and Finance
  – Postal and Shipping
  – Agriculture / Food / Water / Chemical
IT security protection means ……

We need……..

• State-of-the-art IT security defenses for public and private sector enterprises
• Security programs that address implementation of adequate security
• A process for managing IT security risks in a dynamic environment

It’s all about managing risk, not avoiding it.
Information Security Programs

Links in the Security Chain: Management, Operational, and Technical Controls

- Risk assessment
- Security planning, policies, procedures
- Configuration management and control
- Contingency planning
- Incident response planning
- Security awareness and training
- Security in acquisitions
- Physical security
- Personnel security
- Security assessments
- Certification and accreditation

- Access control mechanisms
- Identification & authentication mechanisms (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Boundary and network protection devices (Firewalls, guards, routers, gateways)
- Intrusion protection/detection systems
- Security configuration settings
- Anti-viral, anti-spyware, anti-spam software
- Smart cards

Adversaries attack the weakest link...where is yours?

~ NIST
Network security

• Harden your network and infrastructure assets
• Lower your internet points of presence
• Review and strengthen your firewall rules
  – Don’t allow peer to peer sharing
  – Block known vulnerable ports
• Scan your infrastructure both inside and out
• Review your configurations for obvious vulnerabilities
• Never deploy the out of the box configuration
• Assess new information technologies and systems before deployment to identify vulnerabilities
• Diversify information technology assets
• Reduce information system complexity
• Perform self assessments or audits
More......

- Identify your assets
- Determine the assurance level
- Assess based on the risk level
- Identify your vulnerabilities
- Begin the remediation process
- When connecting system or sharing data ensure you know the security vulnerabilities before you connect

The objective is to achieve visibility into your system security level, develop a plan to remediate and execute on those plans.
Some basic tips

• Develop an enterprise-wide information security strategy and plan aligned with the technology and business strategy
• Get executive buy-in
• Build security in at the beginning
• Establish an assessment/auditing capability
• Harden the target to save money
• Be an informed consumer – steer clear of point solutions for enterprise problems
• Don’t try to boil the ocean. One step at a time
• Manage risk – don’t try to avoid it