The Evolving Security Landscape:
Security and Compliance Trends

Andreas M Antonopoulos
Senior Vice President & Founding Partner
www.nemertes.com
Agenda

- About Nemertes
- Security and Compliance Trends
- Conclusion and Recommendations
Nemertes: Bridging the Gap Between Business & IT

- Quantifies the business impact of emerging technologies
- Conducts in-depth interviews with IT professionals
- Advises businesses on critical issues such as:
  - Unified Communications
  - Social Computing
  - Data Centers & Cloud Computing
  - Security
  - Next-generation WANs
- Cost models, RFPs, Architectures, Strategies
De-Perimeterization

◆ Is that a word?
◆ No, but it’s happening anyway!
◆ You used to have “The Internet Connection” and “The Firewall”
◆ We are rapidly moving to ubiquitous connectivity and mobility
◆ The Internet is everywhere! There is no INSIDE and OUTSIDE in your network
The Changing End-User Landscape

- Employee personal use of technology influences IT decisions for 46% of organizations.
- About 67% of organizations have a formal telework policy.
- iPhone already target of attacks against known vulnerabilities.
- Mobile devices are a significant data loss risk.
- The line between personal and work computing is blurring.
Security by Location

- Most security today is LOCATION-CENTRIC
- Servers and desktops are becoming virtual
- Firewalls, VLANs, ACLs, IP Addresses – Locations
- Location should not be the foundation of your security policy!
Compliance on the Rise

- If Enron gave us Sarbanes-Oxley, what will 100xEnron give us?
- Legislation to pass a national breach disclosure law
- HITECH Act adds more teeth to HIPAA
- PCI-DSS is driving security behavior
- Compliance drives security spending for 37% of organizations
- Compliance requirements will get more prescriptive with sharper teeth
Data-Centric Security

- Data-centric means INSPECTING and PROTECTING the data
- Regardless of where it is
- Anti-malware inwards, data leakage outwards
- Content inspection
- Encryption
- Fingerprinting
- Digital certificates
- Security meta-data
What Should You Be Doing?

**Urgent: Act Now**
- Assess compliance posture against current and future IT environment.
- Perform a gap analysis.

**Short-Term Plans**
- Assess gap analysis and prioritize controls necessary to meet compliance requirements for today and tomorrow.

**Long-Term Plans**
- Implement a continuous compliance process that monitors in real-time compliance posture.

**Specific Needs**
- Determine what’s in-scope and what’s out of scope for compliance and plan separation/isolation of in-scope data.
Compliance Roadmap

- Evaluate current IT environment
- Assume security perimeter is dissolving
- Plan future IT environment
- Assess compliance of both plans
- Perform gap analysis

Urgent: Act Now
Compliance Roadmap

- Assess output of gap analysis
- In-scope versus out-of-scope data
- Work with auditors to prioritize gaps
  - 80/20 rule applies – start with low-hanging fruit
- People, process and technology
Compliance Roadmap

- Process in-place to close compliance gaps
- Regular self-assessment of compliance
- Develop continuous compliance process
Conclusions and Recommendations

- The security landscape is changing rapidly
  - Continually reassess security plans and posture

- Security must match changing enterprise use of technology
  - Assume today’s consumer technology is tomorrow’s enterprise technology

- Inside firewall is “good” … Outside firewall is “bad” … Is 20th Century thinking
  - The dynamics of computing clash with a rigid firewall plan and mindset
  - Emphasis must shift from location-based to user-based security

- Compliance is a driving force in security planning and spending
  - Engage the compliance function early and often
  - Pay particular attention to privacy regulations and legislations
  - Successful compliance requires focus on people, process and technology
Thank You

Andreas M Antonopoulos
SVP & Founding Partner
andreas@nemertes.com