

What About Security?

What do you answer when asked if your network is secure?

*The answer NO leads to CLM (or RGE),
but is YES the Truth?*

What is Security?

The Truth

- Your Network Is NOT Secure!
 - Secure is NOT an End-state i.e. You Are Never “Done”
 - There Is No Absolute Scale
 - It Is Relative To A Specific Business Context
- How Much Risk Do You Want To Take?
 - Security Is About Risk Mitigation

$$\textit{Risk} = \textit{Threat} \times \textit{Vulnerability} \times \textit{Impact}$$

Security Planning: Think Strategically

- A Tradition Of “Technically-led”, IT-based Security Projects With NO Real Business Alignment
- Strategic approach
 - Business Requirements
 - Security Strategies
 - Security Services
 - Security Mechanisms
 - Security Tools & Products
 - Security Operations & Administration



Security Planning: What about Compliance?

1974 – Privacy Act of 1974 (Fair Information Practices)	2000 – Personal Information Protection and Electronic Documents Act (PIPEDA) Canada
1977 – Foreign Corrupt Practice Act (FCPA) SOX precursor	2000 – Children’s Internet Protection Act (CIPA)
1987 – Computer Security Act (NIST role reaffirmed as standard for non-classified Federal data)	2001 – US Patriot Act
1995 – EU Data Protection Directive (Private data)	2002 – Sarbanes-Oxley (Corp governance, reporting)
1996 – HIPAA (Privacy and security of health data)	2002 – Homeland Security Act
1997 – FDA 21 CFR Part 11 (Electronic records/signatures)	2002 – FISMA (E-Govt act)
1998 – UK Protection Act	2003 – Basel II (Europe – Operational Risk)
1998 – Children’s Online Privacy Protection Act (COPPA)	2003 – SB1386 (California Privacy)
1999 – GLBA – (Financial info protection)	2003 – CAN-SPAM (Anti-Spam)
	2005 – AB1950 (Protect personal information)

Should regulations be your primary security architecture driver?

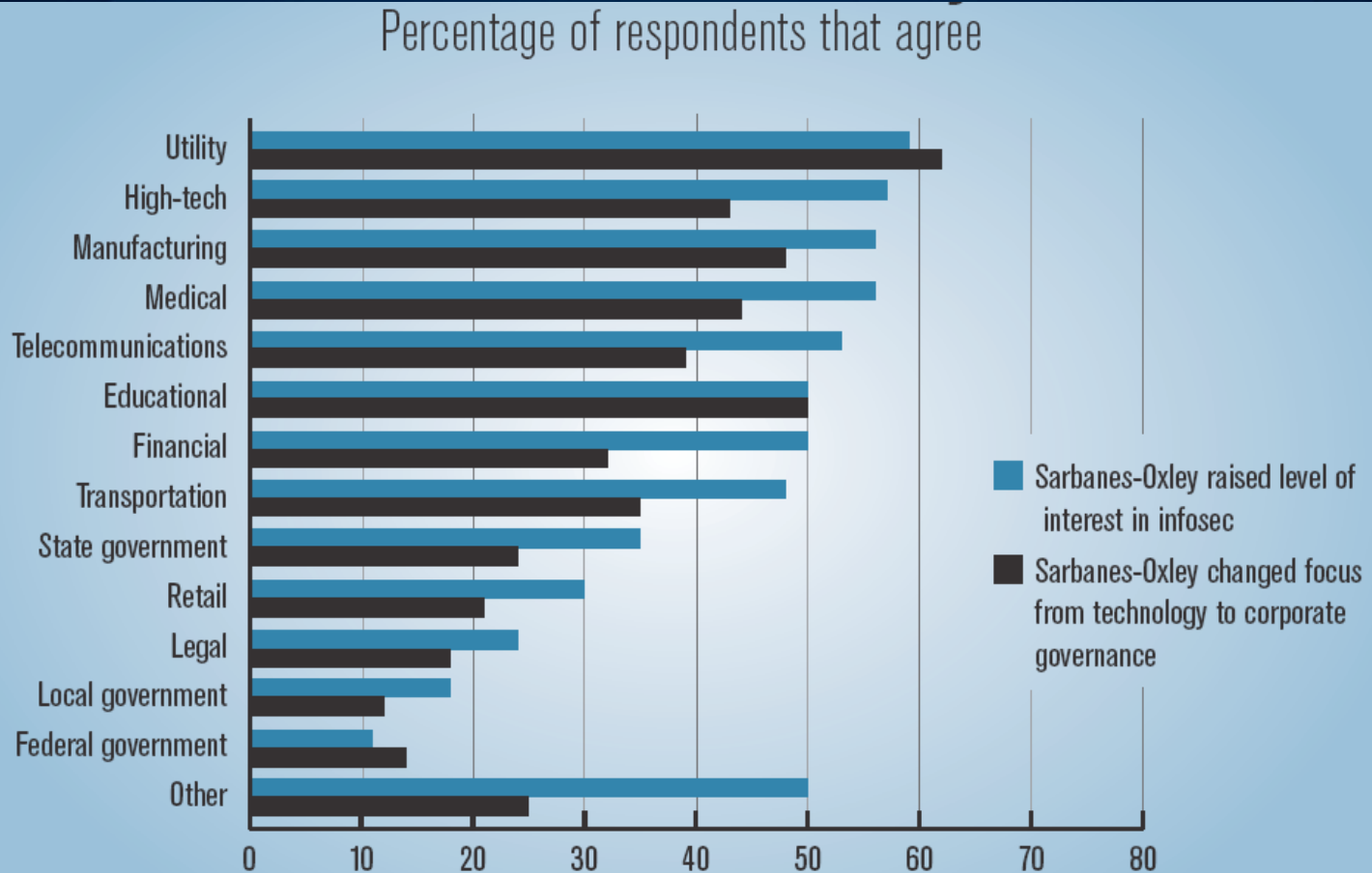
Hint:

SB1386 Has Spawned Over 30 States To Write Individual Variations Of The 1 Law



If You Derive Your Security From Your Business Requirements Your Risk Level Will Be Appropriate

Security Planning: Impact of Sarbanes-Oxley (SOX) Act



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

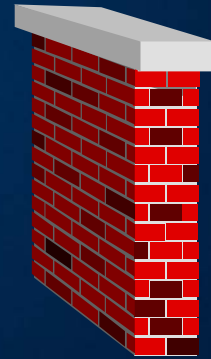
2005: 679 Respondents

Forcing Shift Towards Strategic vs. Tactical Security Approach

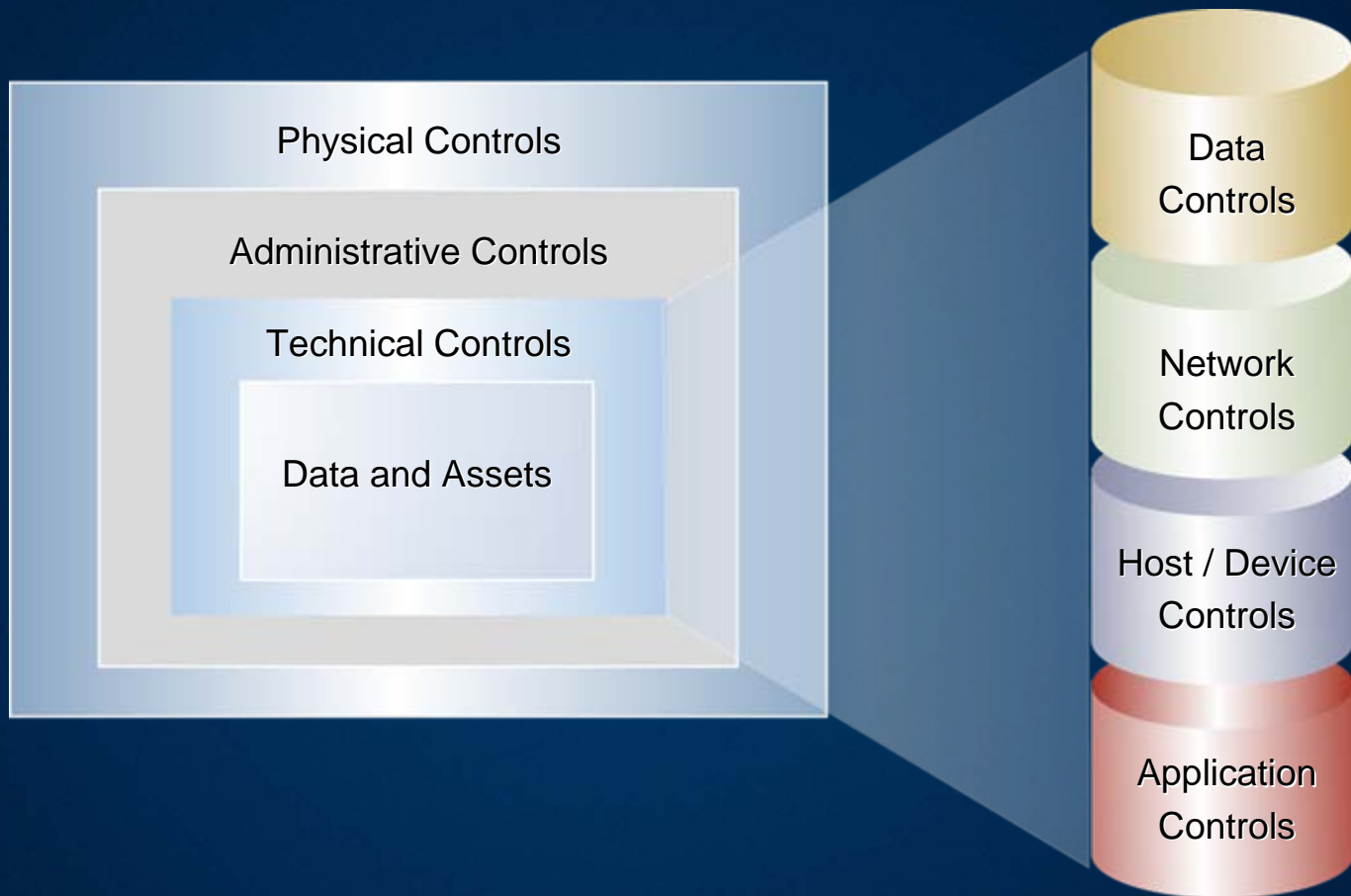
Security Planning: Firewall = Secure?

- Historically, Firewalls Have Been Viewed As:
 - THE Solution To “Bolt On” Security
- What Firewalls Don’t Always Help With:
 - Remote Users
 - Preventing XML Attacks Through Port 80
 - Internal Users
 - ...

There Is No Single Silver Bullet For Security



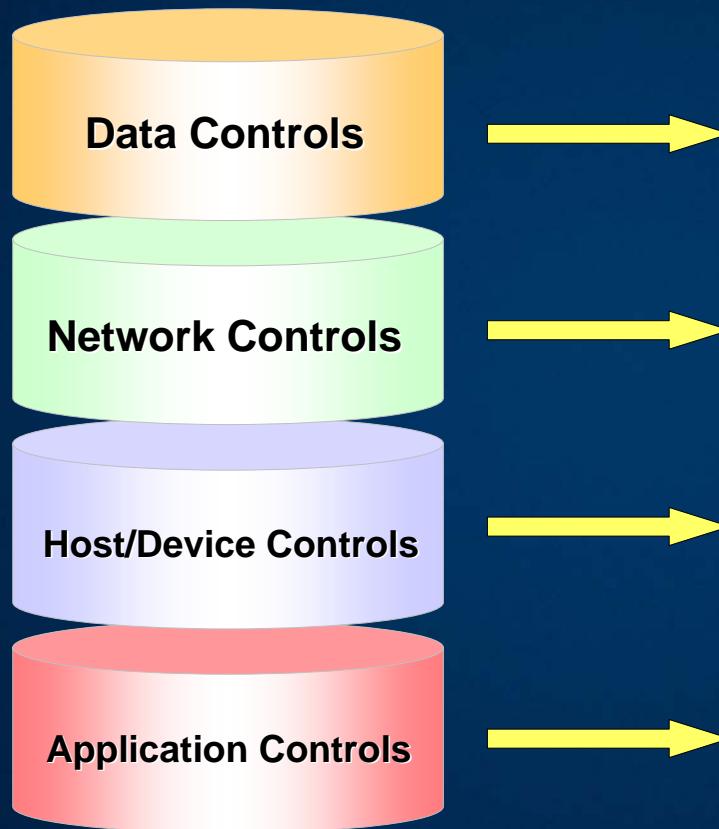
Security Planning: Control Layers



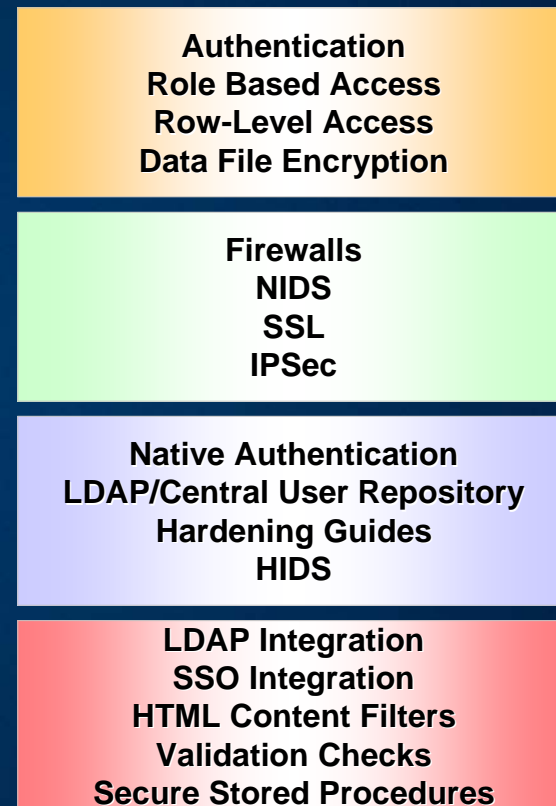
***UC2006 Technical Workshop on Technical Controls For ESRI Products:
"Enterprise GIS: Design – Secure Solutions" - Thurs 8:30am***

Security Planning: Security Mechanisms

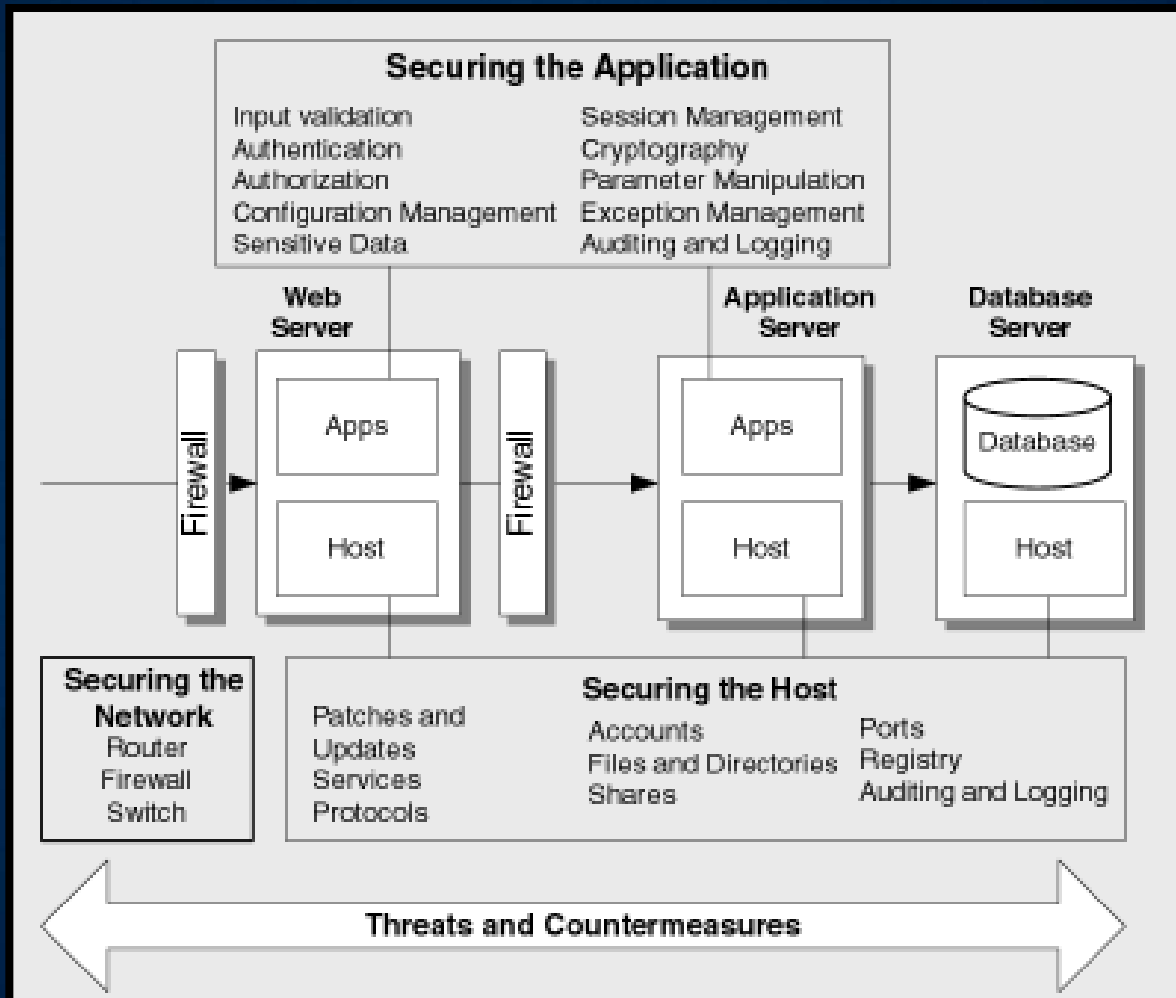
Security Layers



Security Mechanisms



Security Planning: Example Mechanisms



Security Planning: Fundamental Tradeoffs



Security Planning: Best Practices

- ✓ Leverage Your Existing IT Security Architecture
- ✓ Design A Flexible, Scalable Security Solution that allows for Frequent Updates
- ✓ If You Derive Your Security From Your Business Requirements Your Risk Level Will Be Appropriate



Security Planning: Additional Resources

- **New ESRI 2-Day Security Workshop**
 - Available From Professional Services
 - Know Your Options / Best Practices / Emerging Solutions
 - Includes High Level Security Assessment
- Technical Workshop
 - Thursday 8:30am Enterprise GIS: Design – Secure Solutions
- ESRI Whitepaper
 - ***ArcGIS Enterprise Security: Delivering Secure Solutions***
 - <http://www.esri.com/library/whitepapers/pdfs/arcgis-security.pdf>

geography



Questions?