

**International Legal
Technology Association**

Peer Powered

When in Rome, Should You Encrypt as the Romans Did?

South Central Tour: October 4, 5, and 6, 2005

Presented by: Jim Soenksen and Ed Sale



PIVOTGROUP
SOLUTIONS TAILORED, NOT RESOLD.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are detailed with fluted shafts and ornate capitals. The entire slide is framed by a thin brown border.

Presentation Goals

- Define Encryption
- Benefits of Encryption
- Encryption Solutions
- Encryption Selection & Deployment



What is Encryption?

- Process of converting messages, information, or data into unreadable form
 - 1900 BC Egyptian Use
 - Julius Caesar for Government Communication
 - Thomas Jefferson & WW II by US Navy
 - WWII-The Enigma Machine-Germany
 - U.S. Data Encryption Standard
 - PGP
 - Symmetric vs. Asymmetric

The background of the slide features a light blue gradient. On the left side, there is a vertical strip of a classical architectural scene, showing several white columns with ornate capitals, possibly Corinthian or Composite, receding into the distance. The entire slide is framed by a thin white border and a thicker brown border.

Uses of Encryption

- Authentication
- Integrity
- Confidentiality

The background of the slide features a faint, light blue image of classical architectural columns on the left side, set against a light blue gradient background. The columns are detailed with capitals and fluted shafts.

Do I Need Encryption?

- Identify Critical Information Assets-Client Information, Personal Information
- Determine Vulnerabilities/Exposure
- Assess Risk to Firm
- Continue Monitoring, Assessing Exposure & Risk

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are detailed with capitals and fluted shafts, creating a sense of structure and stability.

Encryption Business Benefits

- Protection of the Firms Assets
- Protection of Client's Information
- Regulatory Compliance
- Penalties & Fees
- Firm's Reputation
- Competitive Advantage

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are detailed with capitals and fluted shafts, extending vertically from the bottom to the top of the frame.

Encryption Business Costs and Risks

- Lost Keys = Lost Data
- Reduced Performance
- User Complexity
- Ransomware



Protecting Data at Rest

- Why?
 - To prevent unauthorized exposure of sensitive data
- Where?
 - Individual Files
 - File Systems
 - Databases
 - E-Mail Servers
 - PDAs / Phones
 - Archive Media
 - Laptop Computers
 - Removable Drives



Protecting Data at Rest (cont.)

- How?
 - Individual Files
 - PGP
 - SafeGuard
 - File Systems, Laptop Computers, Removable Drives
 - Windows XP
 - Server 2003
 - PGP
 - Network Appliance
 - Databases
 - DBEncrypt (GreatPlains)
 - nCipher
 - E-Mail Storage (Server and Workstation)



Protecting Data at Rest (cont.)

- How?
 - Archives / Backup Media
 - WinZip (weak crypto)
 - PGP
 - SafeGuard
 - Veritas
 - Additional Technologies
 - Pointsec
 - Trust Digital
 - Enterprise
 - Ensure
 - Absolute
 - F-Secure
 - CompuSec
 - Coreguard



Protecting Data in Motion

- Why?
 - To prevent unauthorized exposure of sensitive data
- Where?
 - In E-Mail
 - File Downloads
 - Remote Access
 - Partner Communication
 - Off-Site Storage
 - Wireless



Protecting Data in Motion

- How?
 - E-Mail
 - PGP
 - CipherTrust
 - Tumbleweed
 - Entrust
 - PostX
 - ZipLip
 - CenturionSoft
 - Zix
 - File Downloads
 - SFTP
 - SCP
 - HTTPS
 - VPN Tunnels



Protecting Data in Motion

- How?
 - Remote Access
 - SSH
 - Citrix
 - VPN Tunnels
 - Partner Communication
 - VPN Tunnels
 - Additional Technologies
 - Apani
 - Cisco
 - Aventail
 - Juniper
 - F5



Public Key Infrastructure (PKI)

- Establish chains of trust
- Authenticate Identities
- Distribute Keys in Certificates
- Key Aging and Revocation

- Major Vendors: Entrust, Cybertrust, Verisign



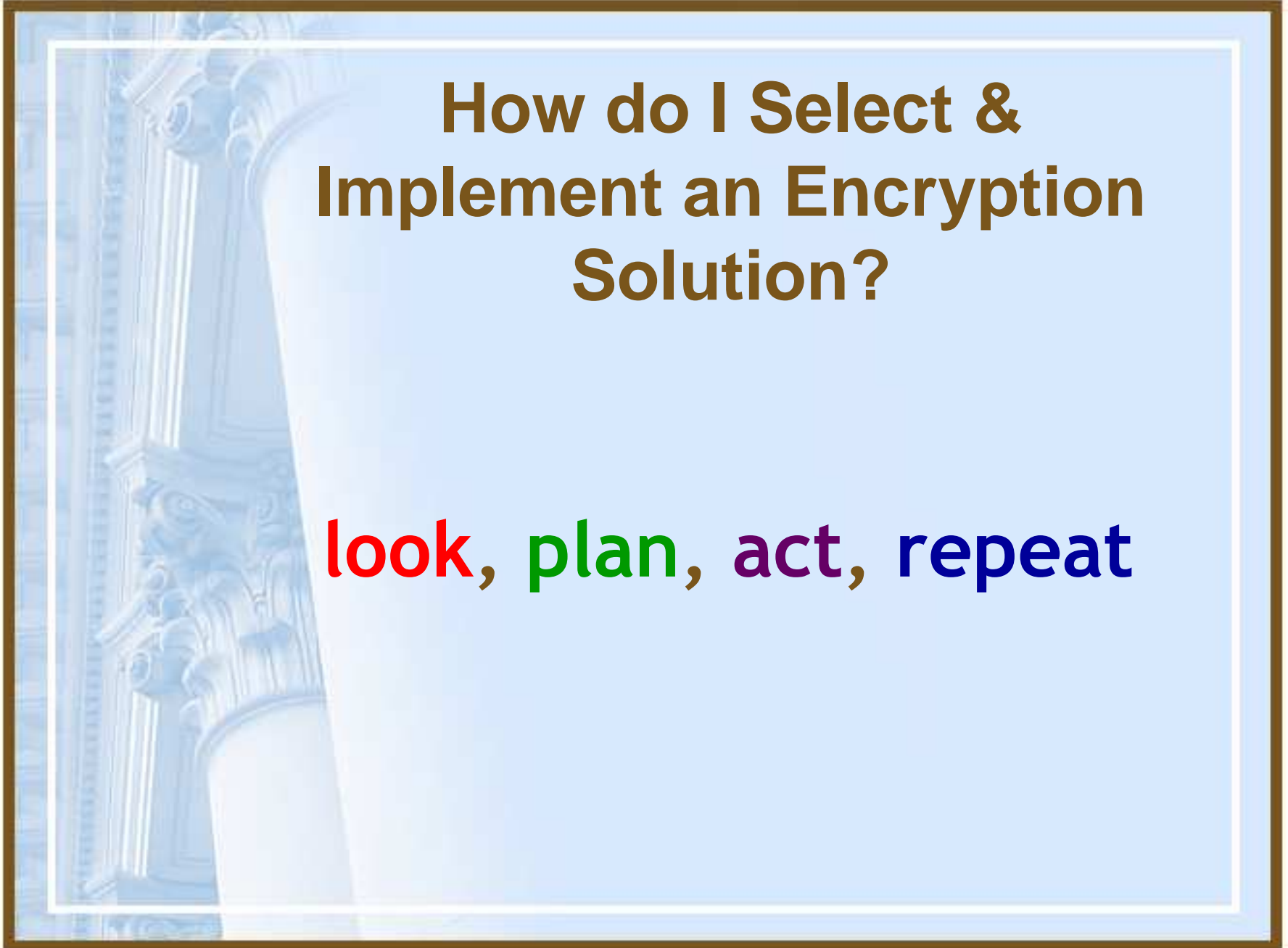
Policies

- What must be encrypted?
- When must it be encrypted?
- How can you monitor/enforce policy?

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are detailed with capitals and fluted shafts, set against a darker blue background.


Training

- Will Encryption be Automatic or Manual?
 - Manual will require user training



How do I Select & Implement an Encryption Solution?


look, plan, act, repeat



How do I Select & Implement an Encryption Solution? (cont.)

look


- Perform Assessment
- Review ID and Access Management
- Review File, Storage, and
- Communication Encryption
- Review Technologies:
 - VPN
 - IPSEC
 - SSL (TLS)
 - Remote Access



How do I Select & Implement an Encryption Solution? (cont.)

plan


- Develop Requirements
 - Data
 - Files
 - Protocols
 - Technologies
 - Policies
 - Training
 - Cost



How do I Select & Implement an Encryption Solution? (cont.)

act

- Trial Implementation
- Test
- Production Deployment
- Training



How do I Select & Implement an Encryption Solution? (cont.)

repeat

- Monitor
- Audit
- Adjust

The slide features a light blue background with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Next Steps

- Risk Assessment
- Develop Encryption Deployment Plan

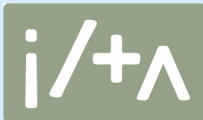
The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Encryption Helpful Sites

- www.cert.org
- www.csrc.nist.gov
- www.sans.org
- www.pivotgroup.net



**What Questions Do
You Have?**



**International Legal
Technology Association**

Peer Powered

THANK YOU

from

Jim Soenksen and Ed Sale



PIVOTGROUP

SOLUTIONS TAILORED, NOT RESOLD.