

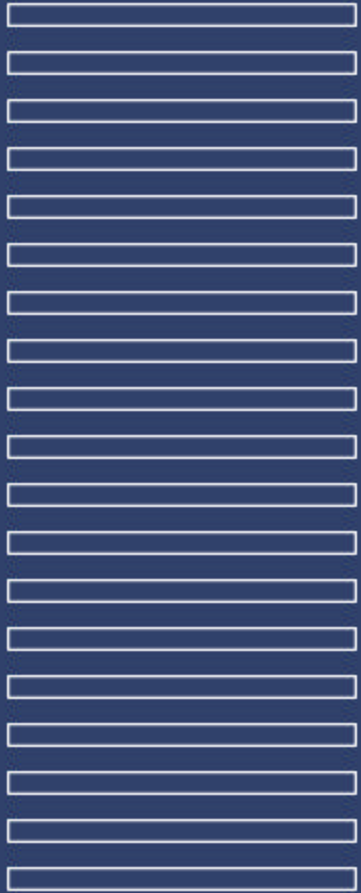


**TUMBLEWEED  
COMMUNICATIONS**

**Compliance Online:  
How to Protect  
Customer Privacy and  
Meet Other Regulatory  
Guidelines**

**ACSAC  
December 12, 2002**

*Ken Beer*



# Agenda

- » What compliance in the world of online messaging really means
  - » A survey of the existing and pending regulations
- » Technology approaches to meet the requirements
- » 3 case studies

# Online Messaging Compliance Issues

- » Practical definition: *A third party (typically the government) must be able to audit a communication trail between two parties*
- » Driven by a need to protect consumers from business misconduct
- » Derived from existing regulations applied to other communication media (e.g. paper)
- » Penalties for non-compliance are effective if harsh and consistent

*Complying certainly benefits your customers, but how much should be invested in compliance processes?*

# A Survey of the Regulations

- » Financial Services/Brokerages
  - » SEC Rule 17a-4
  - » NASD Conduct Rule 3010
  - » Gramm-Leach-Bliley (GLB)
- » Healthcare
  - » HIPAA – Transaction codes, privacy and security surrounding patient healthcare information (PHI)
- » Broad Government Acts
  - » Patriot Act, EU Privacy Act

# Penalties With Teeth

## Breaking News

Posted on Tue, Dec. 03, 2002

The Mercury News

### 5 Wall Street firms fined for not keeping e-mails

**WASHINGTON (Reuters)** - Five Wall Street brokerages, including Goldman, Sachs & Co. , and Citigroup's Salomon Smith Barney, were fined a total of \$8.25 million for not properly preserving e-mail communications, securities regulators said on Tuesday.

While not admitting or denying wrongdoing, the five firms -- Goldman, Salomon, Morgan Stanley & Co. , Deutsche Bank Securities Inc. , and U.S. Bancorp Piper Jaffray Inc. -- agreed to pay \$1.65 million each and will review procedures for keeping e-mails.

“Each firm had inadequate procedures and systems to retain and make accessible e-mail communications,” the SEC, New York Stock Exchange and NASD said in a statement.

“While some firms relied on employees to preserve copies of the e-mail communications on the hard drives of their individual personal computers, there were no systems or procedures to ensure that employees did so,” they said.

Back-up tapes or other formats to keep the e-mails were discarded or recycled “often a year or less after back-up occurred,” they said. In addition to the fines, the firms also agreed to report to the securities regulators on their procedures to comply with the rules for preserving e-mails.

# SEC RULE 17A-4 Requirements

- » Electronic storage media must be “non-rewritable” and “non-erasable”)
- » Make records available for SEC review/auditing
- » Retain an accurate index
- » Keep index available
- » Implement audit software for record input
- » Audit results available to authorized users

# NASD Conduct Rule 3010

- » **Supervisory Systems**
  - » Supervise activity of each registered brokerage representative
- » **Internal Inspections**
  - » Requires implementation of formal review process of communications relating to banking or securities business. Purpose = detecting violations
- » **Retention Program**
  - » Compliance with Rule 3110 and 17a-4...

# Gramm-Leach-Bliley Act

- » Two parts:
  - » Subtitle A: Protection of non-public personal information
  - » Subtitle B: Protection of customer financial information
- » Fines and up to 5 years imprisonment for violations
- » Declarations of privacy policies have already been sent to customers
- » Examples of penalties for non-compliance - TBD

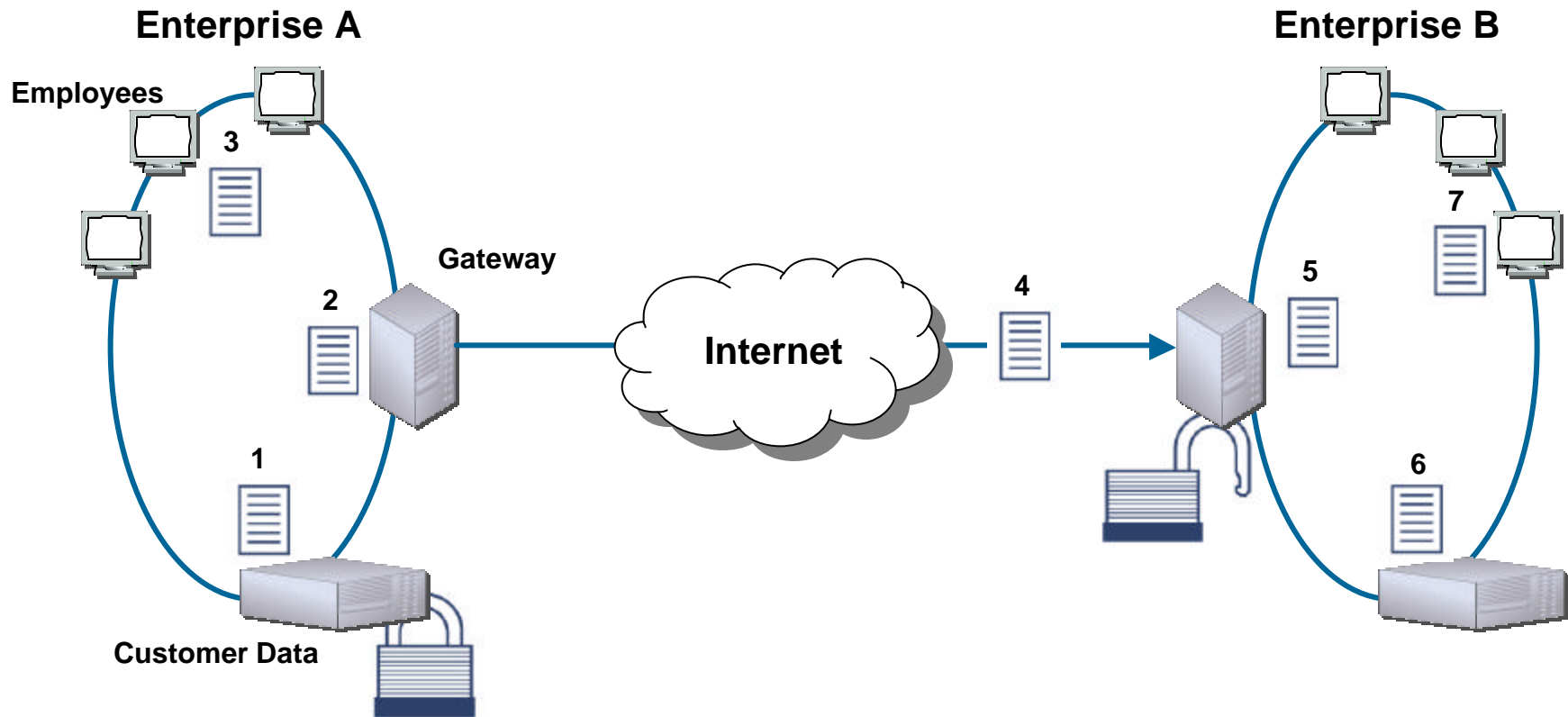
# HIPAA

- » 3-phased enactment of regulations around the storage and transmission of PHI
- » Privacy regulations recently finalized, compliance deadline 4/03
  - » Consent to share PHI both explicitly and implicitly gathered
- » Final security regulations still pending
  - » Will mandate systems in place for encryption, authentication, integrity and auditing of PHI

# Broader Government Regulations

- » Patriot Act
  - » Allows more access for law enforcement to electronic communication archives
- » EU Privacy Directive
  - » Restrictions for use of consumer data within and across country boundaries

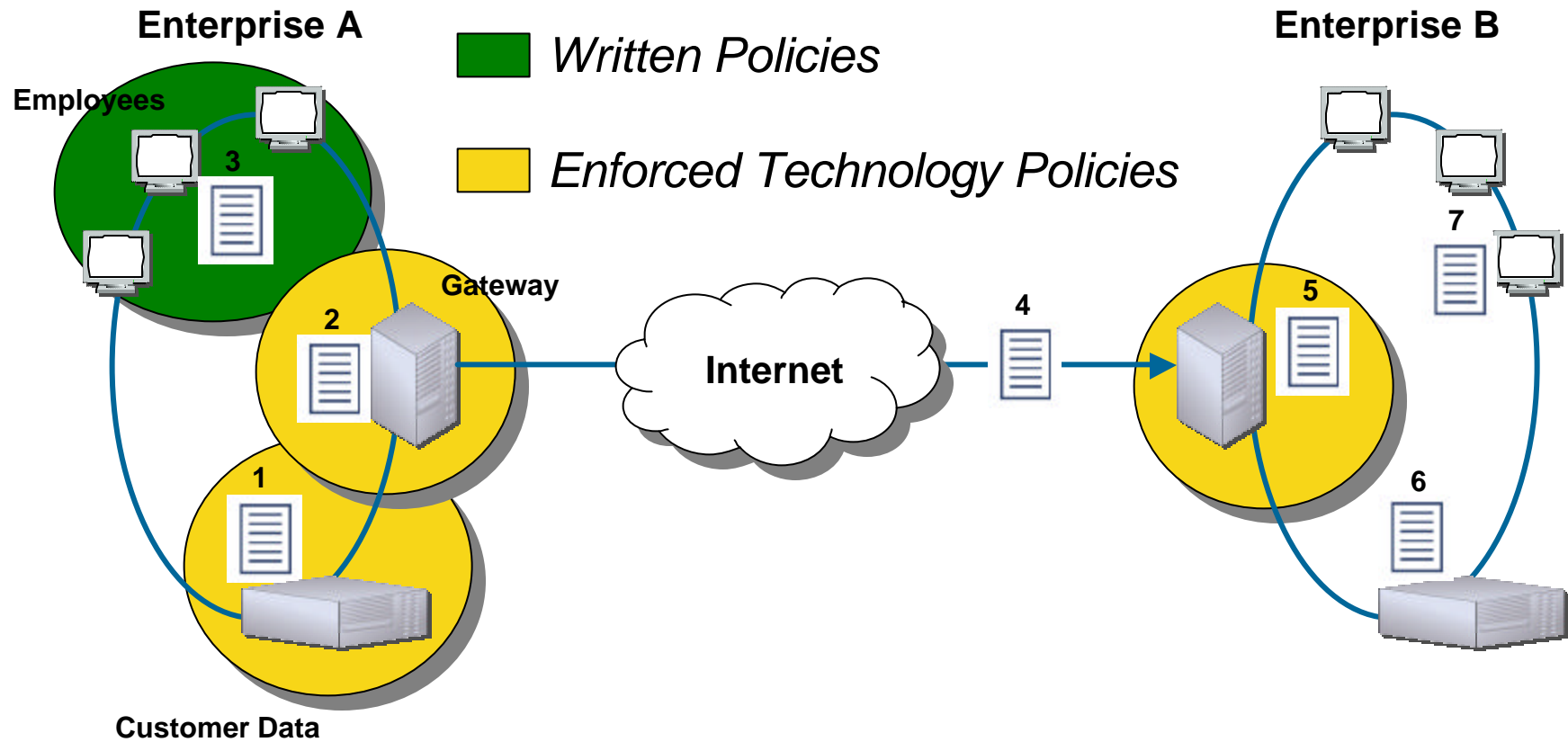
# Multiple Areas of Risk



# Compliance Best Practices

- » *Step 1:* Written policies communicated to employees
  - » Proof of action required
- » *Step 2:* Install monitoring staff, procedures, and technologies
  - » Content filtering at the gateway the only effective solution
- » *Step 3:* Determine appropriate actions for privacy breaches
  - » Showing that you took appropriate action can both prevent heavier fines and future misdeeds by employees

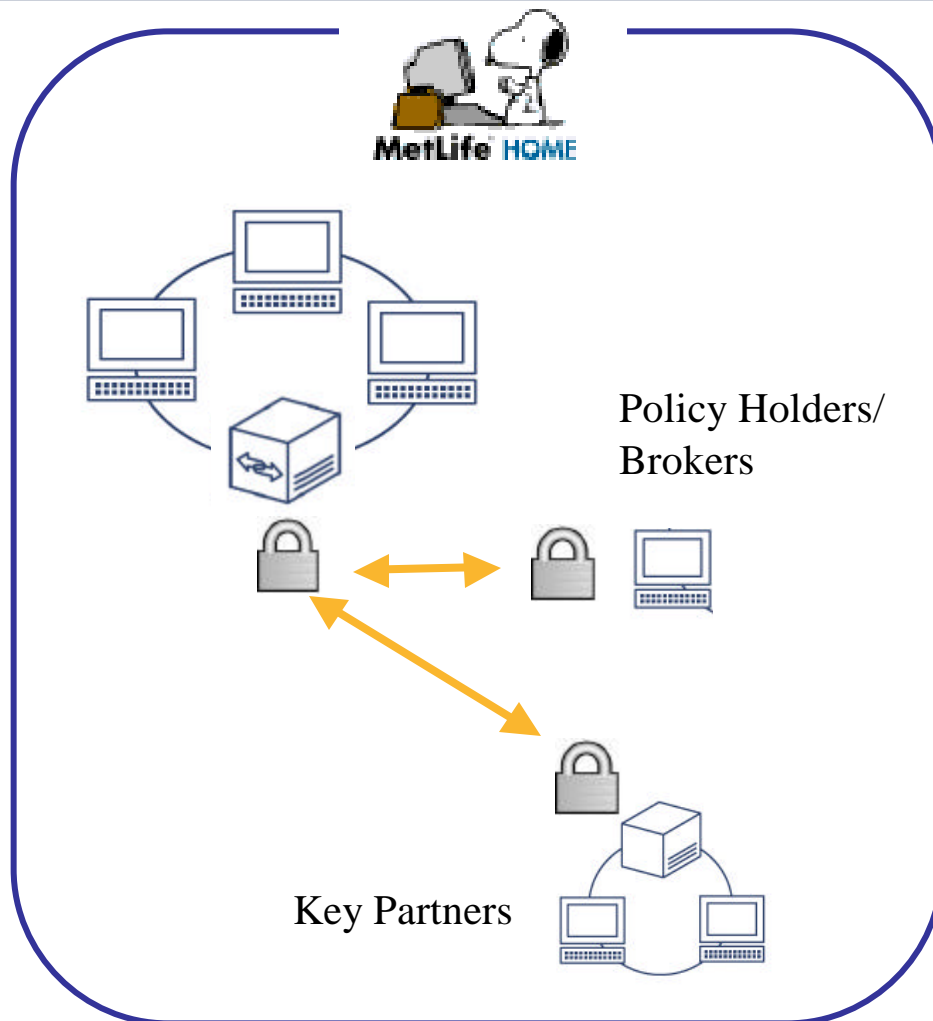
# Where to Apply Technology



# Provide Content Filtering In Order To...

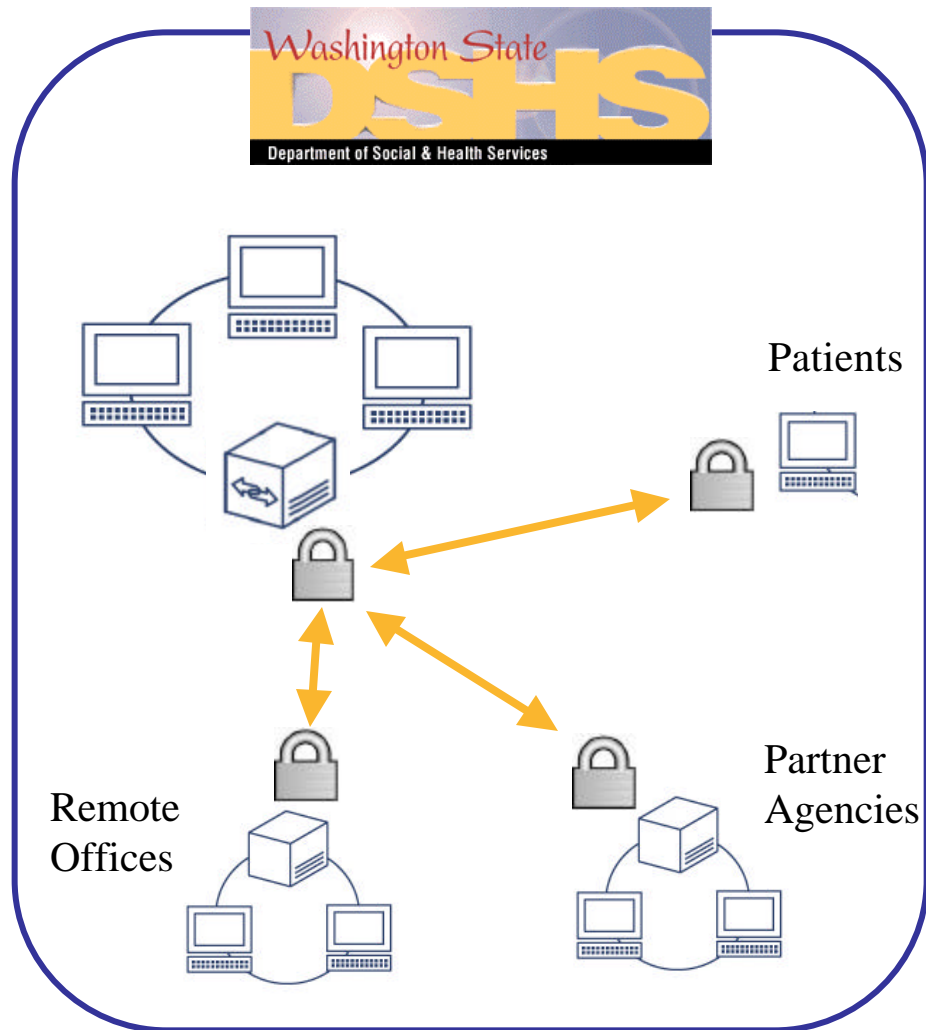
- » Block outbound messages that would violate policy
- » Archive messages from targeted users
- » Encrypt messages that need to be protected
- » Prevent malicious code and spam from being sent or received

# Metropolitan Life



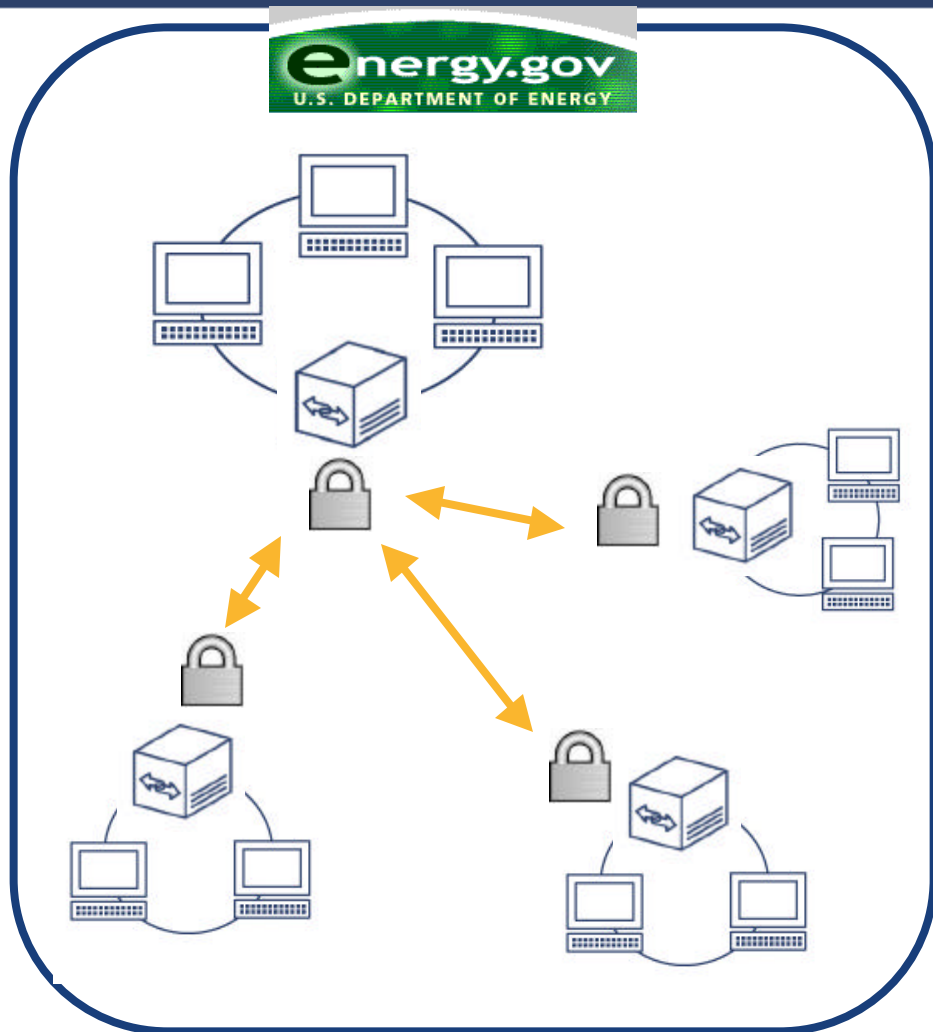
- » Enforce corporate policy and regulatory compliance with message archival
- » Secure e-mail network automatically encrypts messages to/from partner sites
- » A/V and spam protection added benefits

# State of Washington



- » Managing 18,000 email users
  - » Doctors, patients, employers, other agencies
  - » Various technologies available at the desktop
- » Communications scanned for PHI and encrypted as needed
  - » Early mover towards HIPAA compliance

# U.S. Department of Energy



- » Establish secure network between DOE laboratories
- » Email application specific firewall
- » Protect from internal and external threats
  - » IP leaks have national security repercussions

# Summary

- » Evaluate business risks to determine how much to invest for compliance and protection of customer privacy
- » Combine employee training with centralized enforcement at the gateway and other servers