



2006 Best in Show for
Information Security

Automating Compliance and Preventing Data Loss

Today's Topics

- Why Data Privacy is Important
- FTC Guidance – 5 Steps to Protect Your Sensitive Data
- Best Practices for Data Privacy
- Implementing the Solution



Why Data Privacy is Important

- Nearly 40 states have privacy laws similar to California SB1386.
- A federal law is currently making its way through Congress.
- Laws require a company to notify customers or employees if nonpublic personal information about them is lost.
- Over 100 million records containing sensitive personal information have been involved in security breaches since February, 2005.
 - Privacy Rights Clearinghouse - www.privacyrights.org
- Average cost of a data breach to a company is \$182 per lost record (Ponemon Institute Survey)
 - Remediation costs
 - Lost customers
 - Lost market cap



Data Loss and IP Loss Are Significant Risks

“If Phil Howard's calculations prove true, by year's end the 2 billionth personal record -- some American's social-security or credit-card number, academic grades or medical history -- will become compromised, and *it's corporate America, not rogue hackers, who are primarily to blame*. By his reckoning, electronic records in the United States are bleeding at the rate of 6 million a month in 2007, up some 200,000 a month from last year.”

Hackers get bum rap for corporate America's digital delinquency
Peter Lewis _ uwnews.org



Impact of Data Loss

- Increased regulatory oversight and fines for violating privacy laws and regulations
- Customer defections (or loss of potential new customers) due to lack of confidence in security
- Tarnished brand image
- Lost market share
- Remediation costs, including lost employee time to deal with the loss and responding to shareholder and customer lawsuits



Where does the threat originate?

- **74%** of survey respondents said threats to corporate security are now coming from inside the organization.
 - IBM Security Survey 2006
- Up to **70%** of identity theft starts with the deliberate removal of personal data from a company by an employee
 - Professor Judith Collins, Michigan State University
- **Human Error** was responsible for nearly **60%** of security breaches in 2005
 - 4 th Annual CompTIA Study on Information security and the Workforce



In The News

- Over 97 million records containing sensitive personal information have been involved in security breaches since February, 2005.
 - Privacy Rights Clearinghouse - www.privacyrights.org
- Pending termination, AIG employee forwards confidential company information from company email to off-site email and threatens extortion.
 - Law360 January 2007 - www.employment.law360.com
- Deutsche Bank loses position in Hertz IPO after associate sends unauthorized emails to 175 institutional accounts.
 - MarketWatch November 2006 - www.marketwatch.com
- Apple trade secrets and add-on device designs leaked by employees over Webmail.
 - Litigation Alert June 2006 - Fenwick & West
- HIPPA and GLBA regulations set guidelines for protecting sensitive data and enforce encryption standards for healthcare organizations and financial institutions.
- Proposed federal Data Accountability and Trust Act now in Congress.
- Industrial espionage is a booming business.
- SEC SOX regulations require controls on management of soft assets such as customer data and intellectual property.



New Federal Trade Commission Guidance

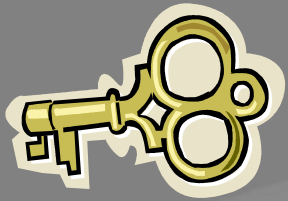
- Federal Trade Commission recently issued guidance on: “Protecting Personal Information: A Guide for Business” (www.ftc.gov/infosecurity)
- FTC’s 5 Recommended Steps to Protect Data
 - Take Stock - know what you have
 - Scale Down - keep only the necessary
 - Lock It - protect data
 - Pitch It - properly dispose of data
 - Plan Ahead - create plan to respond to incidents
- Explicitly recommends two techniques to help companies secure private personal information:
 - Email encryption
 - Content monitoring



Best Practices for Data Privacy

1. Establish Data Privacy Policies and Educate Employees
2. Monitor and Assess High-Risk Data Flows
3. Encrypt Authorized Transmissions of Sensitive Data
4. Block and Quarantine Unauthorized High Risk Transmissions
5. Implement Data Privacy Policies on Endpoint Computers





Best Practice: # 1

- **Establish data privacy policies and educate employees**
 - Categorize and control data based on a “Severity Risk” Model
 - Organized around principle of “potential harm” to a customer/employee if data lost
 - 4 levels of severity and control combinations based on data elements (see next two slides for examples)
 - Educate employees on policies
 - Make sure sensitive information only accessible to those employees who need access to it



Two Types of Information to be Protected

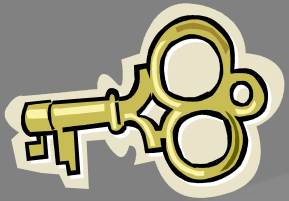
Intellectual Property	Customer Data
<ul style="list-style-type: none">▪ Examples:<ul style="list-style-type: none">▪ M&A plans▪ Financial reports▪ Patent materials▪ Design drawings▪ Source code▪ Multiple document formats.▪ Many languages.▪ Unstructured content stored in file system or content management system.	<ul style="list-style-type: none">▪ Examples<ul style="list-style-type: none">▪ Social security no.▪ Credit card no.▪ Bank account no.▪ Medical diagnostic code▪ Structured data stored in RDBMS or spreadsheet.



Example: Risk Severity Model

Risk Level	Risk Code	Control	Dimension
High (could lead to identity theft)	4	Quarantine	Do not allow any release of data, email, file
Very High (could lead to account takeover)	3	Quarantine Most	If quantity greater than 10, quarantine. If less than 10, release, log and follow detection control procedure. Useful if bank can determine rate of standard transfer; consider programs/other non-standard events that increase files
Moderate (could lead to credit card fraud or SPAM trigger)	2	Release Most & Log	If quantity less than 100, release and log. If quantity greater than 100, release, log and follow detection control procedure
Low/Moderate (could lead to reputation damage; audit comments)	1	Release & Log	Release and log



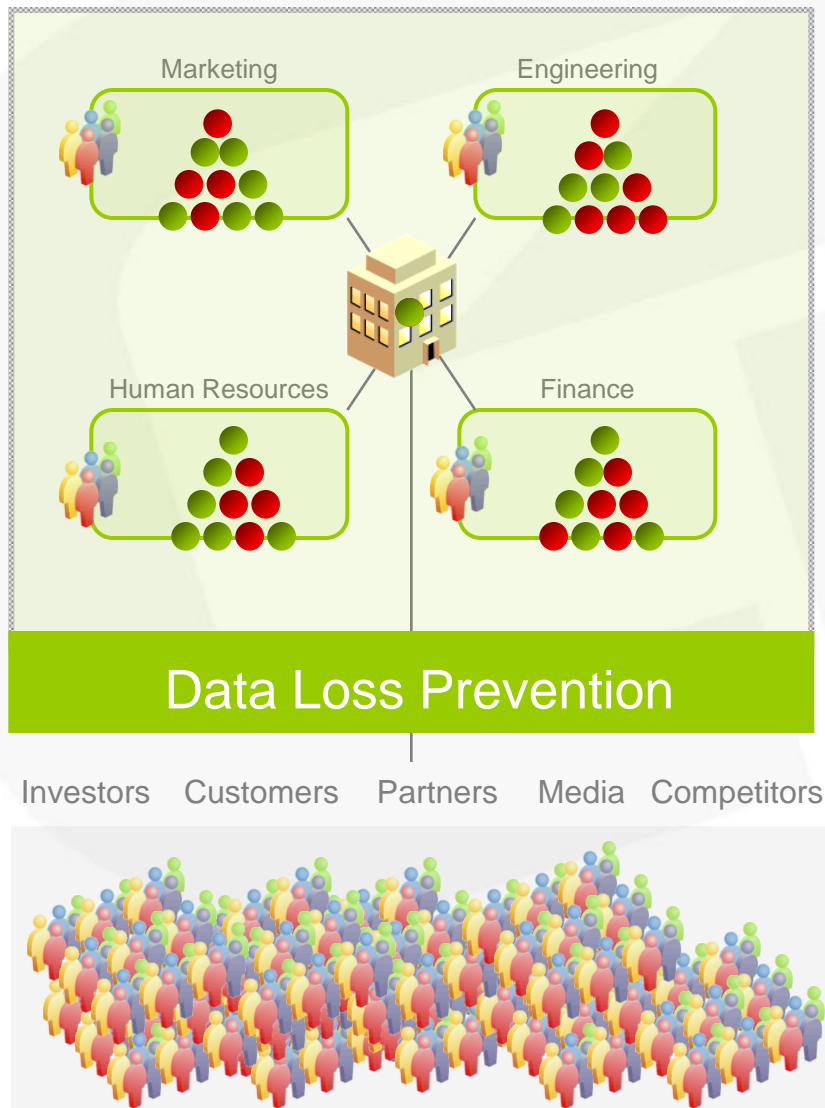


Best Practice: # 2

- **Monitor and Assess High-Risk Data Flows**
 - Monitor electronic business communications to assess the frequency and severity of data leakage
 - Install content inspection appliance at the gateway where an internal computer network joins the Internet
 - Analyze incident records
 - Who is sending data, who is receiving it, when is it sent, what is sent and what channels are used
 - Identify authorized business communications that are candidates for encryption and potential quarantine items

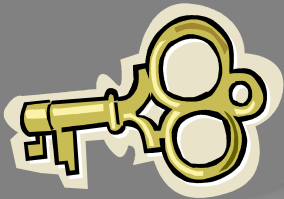


Take Control of Data Transmissions



- Monitor content flows.
- Discover information leaks.
- Implement and enforce automated policies to prevent data loss.
- Educate employees
- Help organisations improve compliance practices.





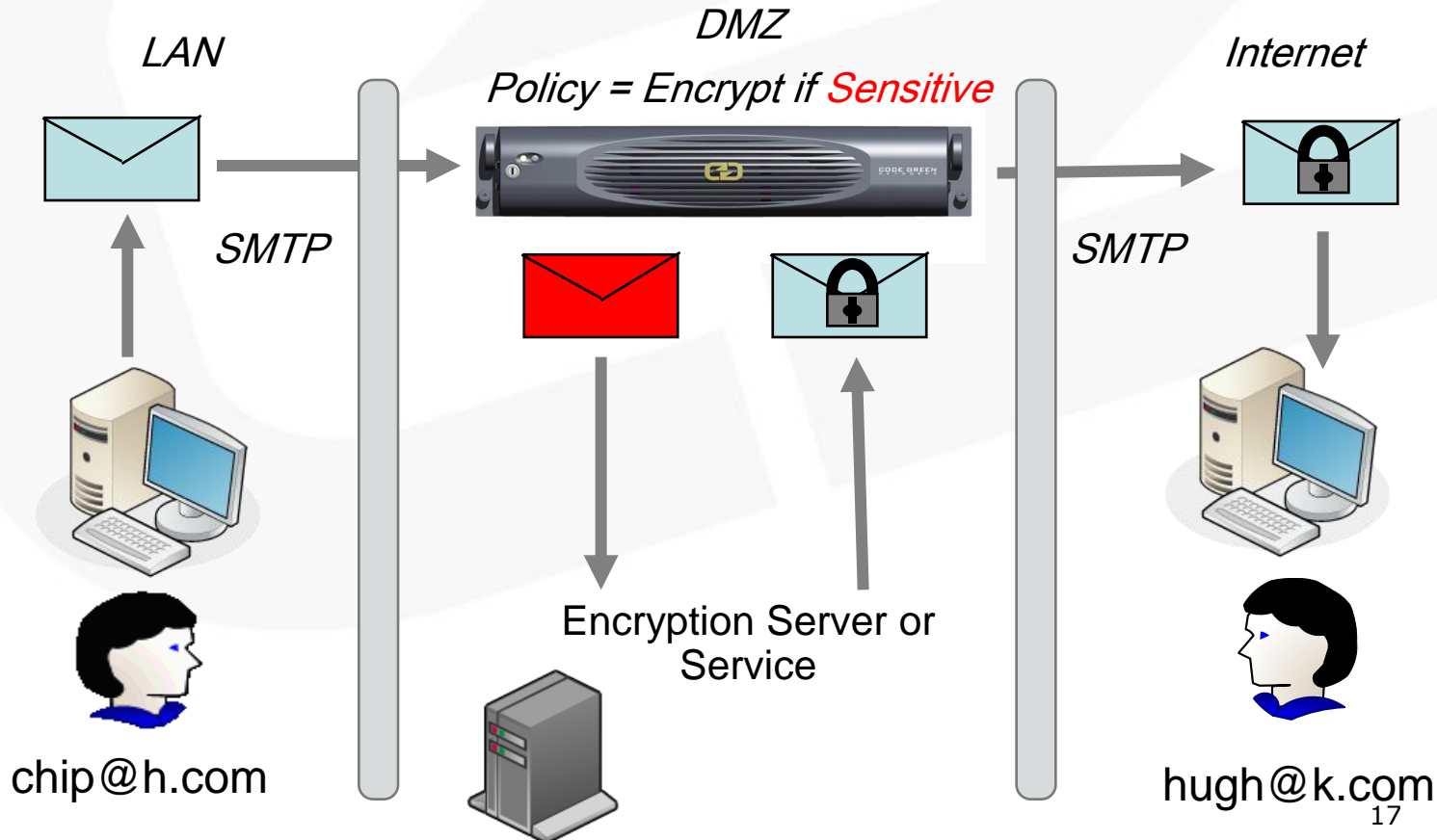
Best Practice: # 3

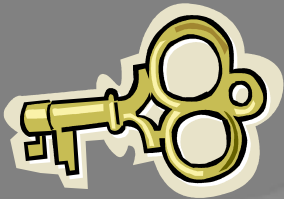
- **Encrypt authorized transmissions of sensitive data**
 - Identify key business communications that may be associated with specific functions and encrypt
 - Customer Service Department communicating with customer via email
 - Marketing sending customer information to outsourced campaign vendors
 - Legal Department filing regulatory compliance documents
 - Operations or IT sending “data dumps” as part of problem resolution process with IT service providers
 - Policy-based encryption enforced at Internet gateway has advantages



Email Encryption: Secure and Protect with a Single Policy

Automate compliance processes by detecting authorized sensitive messages and automatically encrypting them.



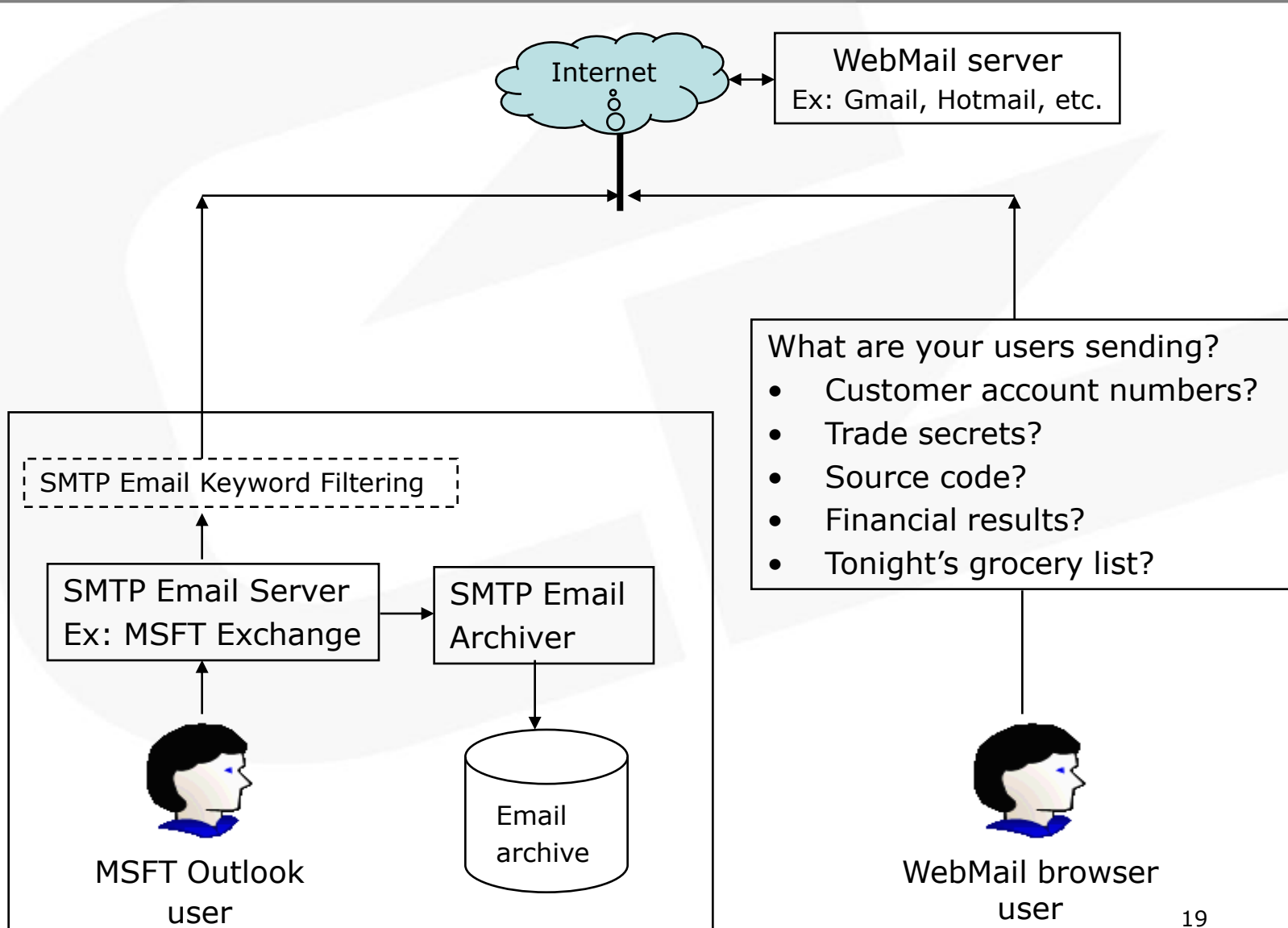


Best Practice: # 4

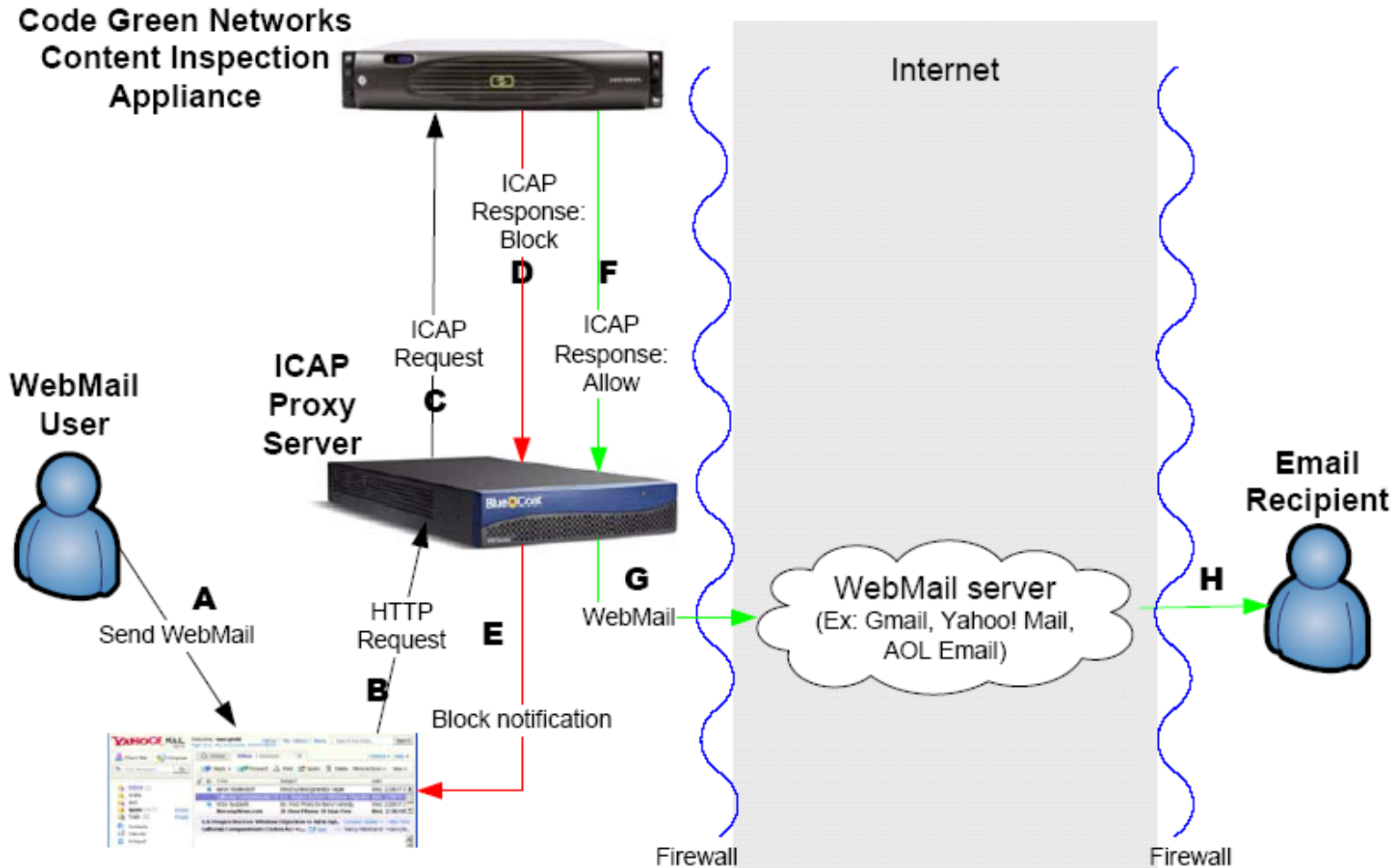
- **Block and Quarantine unauthorized high-risk transmissions**
 - Automate policies to block transmission of Level 3 or Level 4 high risk data
 - Review detailed incident records
 - Assign content “authority” who is tasked with analyzing and resolving data incidents and can authorize transmissions
 - Start with “looser” policies and then tighten

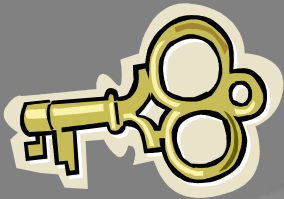


WebMail "Bypasses" Corporate Email Systems



WebMail/HTTP Content Inspection & Enforcement





Best Practice: # 5

- **Implement Data Privacy Policies on Endpoint Computers**
 - In parallel with Internet gateway policies
 - Consider centralized control over USB sticks, iPods, CD-Roms, etc.
 - Endpoint solutions generally require centrally-driven download and administration of client agent software

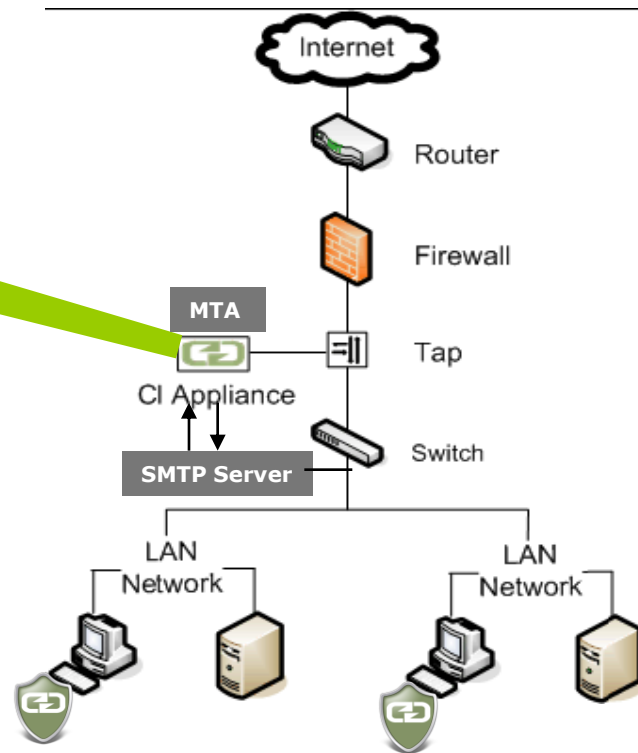


Implementing the Solution



The Content Inspection Appliance is installed at the network gateway and monitors all content flowing to the Internet across all TCP protocols:

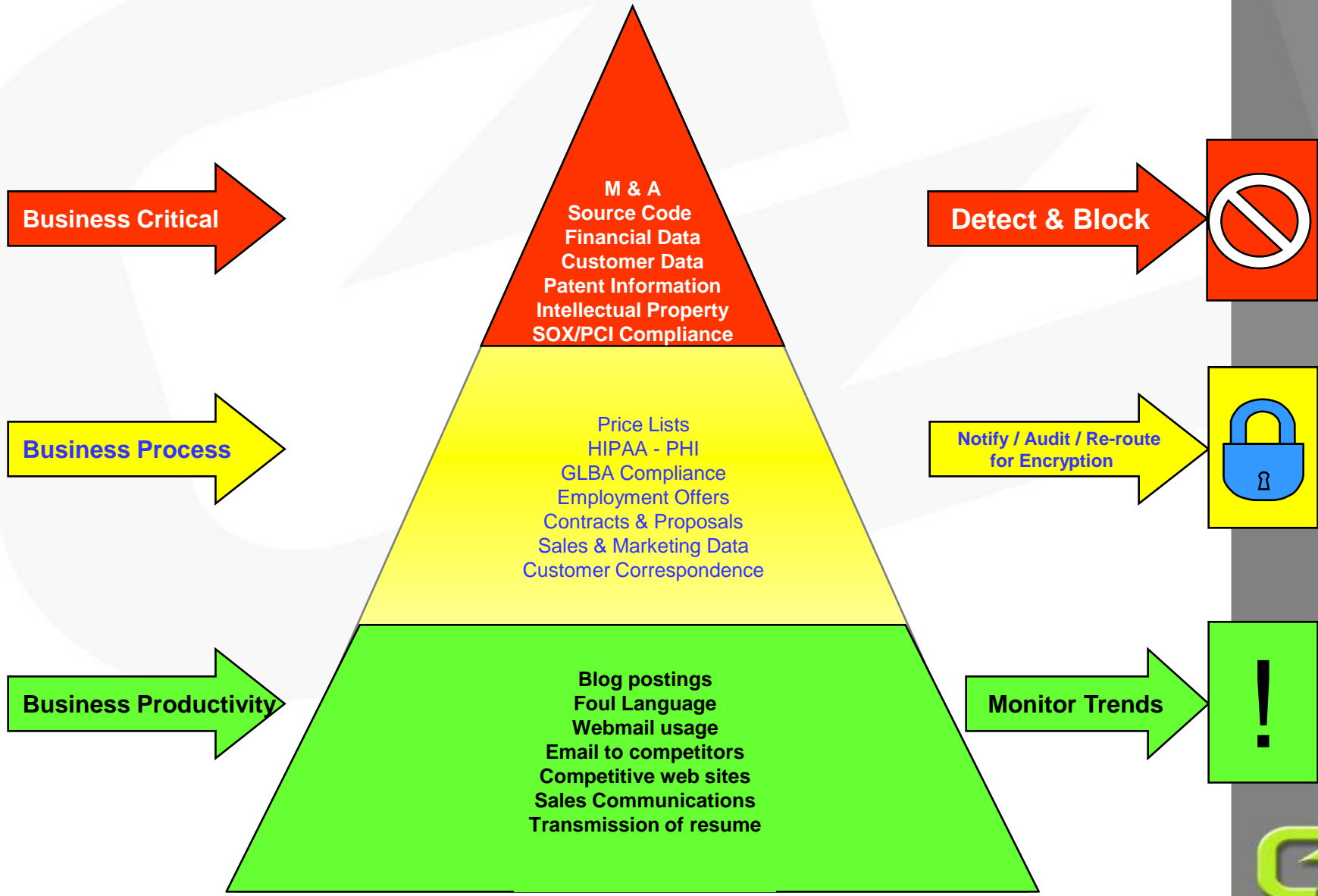
- SMTP Email
- WebMail
- IM
- HTTP
- HTTPS
- FTP



Content Inspection Agents are installed on endpoint machines from a central console and monitor all content copied to/from external devices (ex: USB sticks, CD ROMS)



Improve Business Process & Employee Behavior



Data Loss Prevention Benefits

- Automates compliance to prevent costly and embarrassing incidents.
- Helps identify and fix poor business processes that expose sensitive data.
- Changes behavior of trusted employees to prevent accidental disclosures.
- Prevents industrial espionage.
- Preserves firm's reputation.

"Gartner maintains, however, that the true value (of data loss prevention) lies in helping management to identify and correct faulty business processes and — crucially — identify and prevent accidental disclosures of sensitive data."

**Gartner, Inc., "Magic Quadrant for Content Monitoring and filtering and Data Loss Prevention, 2007", by Paul E. Proctor, Rich Mogull, and Eric Ouellet, April 13, 2007.*



About Code Green Networks

- From the founders of SonicWall
 - Sreekanth Ravi – Founder, Chairman and CEO
 - Sudhakar Ravi – Founder and CTO
- Team of 65 people
 - 35 senior developers with a minimum of 7 years experience each in networking & security technologies
 - The Team has expertise in developing high performance, appliance based content, networking and security products
 - Core development team responsible for SonicWALL UTM technology
- Raised \$32M in equity to date
- Board of Directors includes recognized technology leaders
 - John Roos, CEO Wilson Sonsini
 - Tim Guleri, GP Sierra Ventures
 - Atul Kapdia, GP Bay Partners
- HQ in Santa Clara, CA. Sales offices in United Kingdom, Germany, Norway and Japan.





CODE GREEN
N E T W O R K S

3975 Freedom Circle
Suite 900

Santa Clara, CA 95054
(408) 213-2300

www.codegreennetworks.com