DATA LOSS PREVENTION IN HEALTHCARE

WWT Educational Webinar

November 20, 2008
You can ask questions during the presentation by using the link provided in the Webcast Viewer.
Your Success Drives Ours

- Relentless Focus on People, Process & Partnerships
- Strong Partner Relationships
- Over 1,000 Talented Employees
- Proven Processes
- Nationwide Distribution & Support
- Revenues approaching $3 Billion
- Strong Credit Line - $350MM+
- Key Contract Vehicles: VHA, HPG, ITES-2H, GSA, SEWP
Strong Cisco & Ironport Relationship

- WWT is one of Cisco’s Top 5 Partners.
- U.S. and Canada Theatre Partner of the Year
- Enterprise Partner of the Year
- Federal DVAR of the Year
- Only Gold Partner as Authorized Learning Center
- Over 100 Cisco-certified engineers and more than 500 certifications in advanced Cisco technologies
- Masters Certification in Unified Communication and Security
- WWT was also recognized as a Customer Satisfaction Excellence Partner, the highest distinction a partner can achieve within the Cisco Channel Partner Program
- IronPort Email and Web security solution partner
<table>
<thead>
<tr>
<th>Technology Focus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified Communications</strong></td>
<td>Cisco Unified Communications helps workers increase productivity and collaborate in real-time using their choice of tools and applications.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Best-of-breed security provides rapid response to today’s threats, and offers a path to migration and integration for a holistic, self-defending network.</td>
</tr>
<tr>
<td><strong>Data Center</strong></td>
<td>Information is your most valuable asset. Maximize your data through integrated hardware, software, and services.</td>
</tr>
<tr>
<td><strong>Wireless</strong></td>
<td>Evolve your wireless network with the Cisco Mobility Services Engine and a suite of mobility services software.</td>
</tr>
</tbody>
</table>
Cisco Data Loss Prevention Solution

November 20, 2008
Panelist:

- Juanita Logan, WWT Healthcare Business Dev. Manager
- Ashish Upadhyay, WWT Security Business Dev. Manager
- John Quinn, Cisco/IronPort Channel Manager
- Sarah Schultz, Cisco Security Solutions
- Scott Maxwell, Cisco Security Channel Manager
- David Harrison, CCIE # 8521, WWT Security Lead Engineer
- Ladi Adefala, WWT Security Practice Manager
Agenda

What is Data Loss Prevention?

What is the Cisco Data Loss Prevention Solution?

How do Data Loss Prevention Products Work?

What are my Next Steps?
Q: What is Data Loss Prevention?
What is Data Loss Prevention (DLP)?

- Data Loss Prevention is:
  - A business solution that requires a comprehensive strategy
  - Technology that inspects sensitive content, and audits and enforces content use policies

- DLP can be used for:
  - Regulatory due diligence
  - Intellectual property protection
  - Acceptable use enforcement
  - Identify theft, data theft, accidental data loss…
Q: Why do I need Data Loss Prevention?
The Evolution of Security Threats

Today’s Work Environment Is Changing

Collaboration a Competitive Advantage

Regulatory and Corporate Governance Pressures

More Data Is Lost/Stolen*

*Attrition.org Data Loss Archive and Database
Q: What's the big deal about DLP? Why are so many companies planning to deploy it?
Details of 25 million child benefit recipients have been lost after two discs containing the data were sent from HM Revenue and Customs to the National Audit Office (NAO) but appeared not to arrive. The data included details of millions of bank accounts.

11/20/2007

Confidential records from more than 40 global businesses were stolen and stored on an unprotected server by a Russian cyberthief. The files came from Germany (621), France (322), India (308), Great Britain (232), Spain (150), Canada (86), Italy (58), the Netherlands (46), and Turkey (1,037), among others.¹

5/2008

¹ Computerweekly.com
Accidental Data Loss

Prevent Sensitive Data from Being Transferred to Removable Media, Such As Thumb Drives, USB Sticks, or CDs

Scenario

A UK-based healthcare organization reported a member of staff losing a USB memory stick containing data extracted from the medical records of 4000 patients. Data consisted of the NHS number, customer identification number, first and second name, date of birth, sex, condition, GP code, practice code, and GP name.

December 2007 http://news.bbc.co.uk

Cisco Solution

- Cisco Security Agent can prevent files containing sensitive data or sensitive keywords from being copied to removable media, such as a USB stick
- Cisco NAC can prevent unauthorized access to the network containing the sensitive databases
The Disgruntled Employee

Prevent Sensitive Data from Being Copied and Pasted to External-Facing Applications, Such As Blogs, Social Networking Sites, or Instant Messaging

A US-based healthcare organization informed 140 of their insureds that a former employee posted personal information such as names, addresses and telephone numbers, as well as medical record numbers and some routine lab information on her blog. This organization was one of the first to be fined for violating HIPAA by the California Department of Managed Health Care (DMHC).

March 2005 www.computerworld.com

Cisco Solution

- Cisco Security Agent protects against Clipboard abuse, whether intentional or accidental, when sensitive data is cut, copied, pasted to an external Website (such as blogs or Facebook) or Instant Messenger
The Negligent Employee

Scenario

A vulnerability analysis at a major southern California hospital revealed that doctors were able to log into their hospital desktop computers from home via an Internet available RDP connection (no VPN) and were able to view patient information over an unencrypted channel.

October 2005 (Private Communication with Author)

Cisco Solution

- Cisco Adaptive Security Appliance supports SSL and IPsec VPNs to authenticate and encrypt communication channels for remote access users
- Cisco Secure Desktop is available for use with Cisco SSL VPN to prevent data loss through:
  - Checking endpoint location/security posture before remote connections are established
  - Encrypting file downloads during a session
  - Providing post-session clean-up, e.g. deleting temporary files, internet history, and auto-complete p/w’s
- Cisco NAC tightens the security policy by enforcing that all computers connected to the network via VPN are company-controlled computers and meet company’s security policies
The “Oops” Email

Accidental Data Loss Over Email Can Occur Simply by Using Outlook’s Auto-Complete

Scenario

A large pharmaceutical company’s outside lawyers mistakenly emailed confidential merger discussions to a reporter rather than their co-counsel (with the same last name), costing the organization nearly $1 billion.

January 2008 http://www.portfolio.com

With IronPort C-Series

- Enforce email communication between authorized parties with policy-based encryption, including user authentication and key delivery
- Recall email if it is inappropriately delivered to the wrong business partner with the Email Recall feature
- Monitor and block emails containing sensitive keywords, so that a document filled with critical data types sent to a non-business partner triggers a DLP violation
Employees Engage in Risky Behavior in Regards to Corporate Data

Unauthorized application use: 70% of IT say the use of unauthorized programs result in as many as half of data loss incidents.

Misuse of corporate computers: 44% of employees share work devices with others without supervision.

Unauthorized access: 39% of IT said they have dealt with an employee accessing unauthorized parts of a company’s network or facility.

Remote worker security: 46% of employees to transfer files between work and personal computers.

Misuse of passwords: 18% of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.
Q: What do Data Loss Prevention products really do?
Data Loss Addresses Key Areas of Risk

- **Data-In-Motion**
  - Email, IM, Web, FTP, Wireless
  - Monitor for sensitive information and acceptable use
  - Encryption
  - Conditional blocking
  - Employee Education
  - Control of rogue communications

- **Data-at-Rest**
  - Storage, Databases, Tapes
  - Encrypt tapes or storage
  - Prevent unauthorized access to back-end systems

- **Data-In-Use**
  - Endpoint
  - Prevent sensitive information from leaving (i.e. USB)
  - Offline protection
  - Employee Education

- **Compliance Regulations**
  - PCI - Customer credit card information
  - HIPAA - Medical Information
  - GLBA - Financial Information, etc
Q: What are the top areas of data loss risk?
IT's #1 Concern Over How Corporate Data Is Leaked or Stolen

InsightExpress Survey, 2008 Commissioned by Cisco

Among IT Decision Makers

- Portable USB drives: 33%
- Email: 25%
- Stolen laptops: 11%
- Lost laptops: 8%
- Verbal communication: 8%
- Instant messaging: 4%
- Other: 3%
- Don't know/Not sure: 8%
Q: What is a Cisco Solution in the DLP space compared to other vendors?
DLP Market—Overlay vs. Integrated

**Overlay DLP**

- Pure-Play Vendors – DLP as Standalone Implementation
- Involves All Major Channels of Leakage (Gateway, Endpoint, Encryption)
- Single Policy Framework and Management
- Typically Fortune 500 or Regulated Organizations ($1M+ Costs)
- Monitors and Process Content at All Data Points
- Attains Bulk of Analyst Attention—Revolution Strategy

**Integrated DLP**

- Security Vendors – DLP Integrated into Security Devices
- Addresses Highest Points of Risk (or Biggest Sources of Leaks)
- Embedded into Existing Security and Network Infrastructure
- Applicable for Enterprise and Mid-Market Companies (Sub-$1M Costs)
- Entry into Gaining Visibility into Data Loss Points
- Minimal Analyst Attention—Evolution Strategy
What is Cisco Data Loss Prevention?

- A comprehensive strategy for preventing confidential and private data loss, including:
  - Accessing risk to recommend the right strategy for preventing data loss - includes people, process, and technology
  - Enforcing content policies to prevent critical data loss at high-risk points, over email and at the endpoint, with IronPort C-Series and Cisco Security Agent
  - Securing data from other avenues of risk
CSA 6.0 Data Loss Prevention
Identify and Control Sensitive Information

- Classification
  - Credit card, Social Security #s
  - Intellectual property definitions

- Reporting
  - Track the location and usage of sensitive data

- Enhanced user education
  - Query user and audit

- Updated enforcement controls
  - Block printing
  - Flexible clipboard control
  - NAC quarantine

Tag | Pattern
--- | ---
<confidential> | confidential
<credit_card> | @credit_card
<source_code> | #include <
<SSN> | @ssn

Discover

Monitor

Educate

Enforce
IronPort Data Loss Prevention
Reduces Complexity
Q: What are the key points of integration between DLP and other technologies that I might already have in place?
**Cisco ASA with SSL VPN**
- ASA: QoS filters to block sensitive files
- SSL VPN: Authenticate and encrypt remote connectivity
- SSL VPN: Cisco Secure Desktop to protect and clean-up after remote interactions

**IronPort**
- Prevent Data Loss at Network Perimeter
- Enforce company policy before sensitive information leaves
- Encrypt mail when/where necessary

**NAC Appliance**
- Ensures CSA running
- Verifies connections via VPN are from company-controlled computers

**Cisco Security Agent**
- Scans and can tag data files for sensitive data
- Prevents copying to external media (USB, dvd, etc)
- Prevents using with (inter)network applications (e-mail, IM, browser)
- Prevents bypass of IronPort network protection
- Enforce VPN while off network
## DLP Solution Differentiation

<table>
<thead>
<tr>
<th>Type</th>
<th>Solution</th>
<th>Vendors</th>
<th>Provides Additional Value</th>
<th>Price</th>
<th>Complexity</th>
<th>Customer Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overlay DLP</td>
<td>Cover everything</td>
<td>DLP Pureplays</td>
<td>No</td>
<td>$$ $$</td>
<td>High</td>
<td>200-500*</td>
</tr>
<tr>
<td>Integrated DLP</td>
<td>Largest Pain Point</td>
<td>CSA, IronPort</td>
<td>Yes (Security)</td>
<td>$</td>
<td>Low</td>
<td>Thousands</td>
</tr>
</tbody>
</table>

*Burton Group Estimate*
Q: What are the basic steps to implementing DLP?
DLP Solution Components

1. Where is Your Risk?
   - Information audit to find out how organization uses sensitive data

2. What are your Social Factors?
   - Distributed sites? Global? Social behaviors?

3. Define Functional Solution
   - Enforce of Content Policies over Email or Endpoint
   - Secure Wireless
   - Protect Remote Workers
   - Control Access to Networks, Databases, and Applications
   - Monitor Physical Access
   - Encrypt Data-at-Rest
   - Granular Policy Management
   - Information Leakage / Web App Protection

4. Implement Data Loss Prevention Policy

To Protect Against Data Loss, a Multi-Layered Strategy Is Needed
Q: Can you help to better understand HIPAA compliance requirement related to DLP?
HIPAA – What Does it Require?
42 HIPAA Audit Questions from Piedmont Hospital

Technology Questions can be grouped into 8 categories

1. User Authentication, access rights, termination
2. Transmission and encryption
3. Network Security - Preventing, detecting, containing and correcting security violations (incident reports)
4. Logging, tracking, monitoring
5. Remote Access
6. Wireless Security
7. Anti-virus & Patch Management
8. Database Security

Source: ComputerWorld June 19, 2007
Cisco Self-Defending Network Solution for HIPAA Compliance

Category 1
Category 2
Category 3
Category 4
Category 5
Category 6
Category 7
Category 8
Case Study
CA Dept. of Alcohol and Drug Programs
Data Loss Prevention via IronPort’s Email Security Appliances

ADP’s Challenge

- Local Government mandated outbound content filtering
- Encryption to meet patient privacy and similar regulations
- Prevent accidental disclosures of confidential records data, including patient records
- Secure messaging with outside partners
- Other needs: phishing protection, easy message retention, improved system management

IronPort Solution

- IronPort C-Series email security appliance
- Email Encryption Envelope Server, IronPort Anti-Spam, IronPort Virus Outbreak Filters, Sophos Anti-virus
- Rapid deployment of Data Loss Prevention technology
- Ensures compliance with compliance laws
- Set and forget management; little to no administrative intervention
- Industry leading anti-spam and anti-virus protection at the network perimeter, providing a first line of defense for Exchange servers

“...The selection of the IronPort email and encryption system fulfilled the need for a secure electronic messaging system as the department requires a secure transmission method to meet HIPAA guidelines as well as other administrative requirements...”

Gary Hummel
CISSP Information Security Officer
Dept. of Alcohol and Drug Programs
Q: How can the data be controlled and protected?
Data Loss Prevention Foundation

Integrated Scanning

Integrated Scanning Makes DLP Deployments Quick & Easy
Data Loss Prevention Foundation
Integrated Remediation

Remediation: Encryption
Remediation: Notification
Remediation: Reporting
Remediation: Quarantine

Integrated Remediation Eases Work Flow Burden
Cisco Security Agent 6.0
Sample DLP Controls

- Controls for USB drives, CD, iPod
- Monitor usage
- Confidential file controls
- Authorized user controls
- Location-based controls

End user Business Justification for audits
Consolidated event reporting of USB usage
Q: You mentioned that an important part of DLP is managing people. How can we better educate our employees?
Recommended Practices for Preventing Data Loss

“Data protection requires teamwork across the company. It’s not just an IT job.”

—John Stewart, Cisco Chief Security Officer

Recommended Practices

1. Know your data
2. Tell employees to treat data as if it’s their own
3. Think globally, act locally
4. Foster an open environment between IT and employees
Q: What are the key takeaways from today’s session?
Data Loss Prevention Summary

- Data loss instances are increasing, and there are many ways to lose patient data in today’s environment.
- WWT can recommend a comprehensive strategy to address all avenues of data loss, which includes people, process, and technology for the highest points of risk.
Q and A
More Information

- Cisco.com Data Loss Prevention site
  www.cisco.com/go/dlp

- Information on global data breaches
  http://www.privacyrights.org/ar/ChronDataBreaches.htm
  http://attrition.org/dataloss/

- Legislation on data privacy laws (US only)
  http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm
Thank You For Your Time

Please take a moment to complete the evaluation

The archive of this event will be available in two business days.

The final QA document as well as an MP3 download will be accessible in the archive.
DATA LOSS PREVENTION IN HEALTHCARE

This Presentation Has Ended. Thank You for Participating