RSA
The Security Division of EMC

The Truth about Data Loss

Kelvin Wee **CISA**, **CISM**, **CISSP**
Principal Consultant – (DLP Specialist)
Asia Pacific and Japan
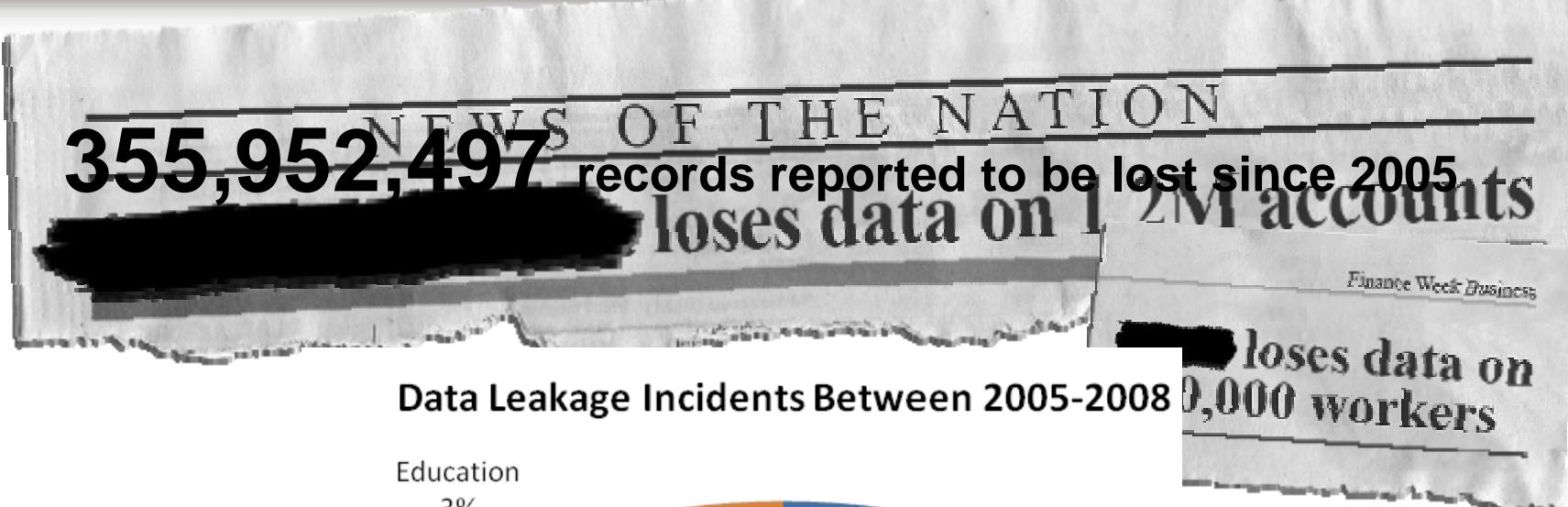
# RSA Data Loss Prevention

Data Breaches Overview

RSA DLP Solution

Five Critical Factors

2

What's Happening To Customer / Employee Data

355,952,497 records reported to be lost since 2005

NEWS OF THE NATION

loses data on 1.2M accounts

Finance Week Business

loses data on 0,000 workers

Data Leakage Incidents Between 2005-2008

Education 3%

Healthcare 8%

Tech & Manufacturing 19%

Other 13%

Retail 35%

Hospitality 22%

Source: Privacy Rights Clearing House, Data Loss Database, RSA Research & Analysis

RSA
The Security Division of EMC

Information Leakage

BBC NEWS | Technology | Workers 'stealing company data' - Windows Internet Explorer

http://news.bbc.co.uk/2/hi/technology/7902989.stm

Live Search

BBC NEWS | Technology | Workers 'stealing com...

Page ▼   Tools ▼

BBC

Low graphics | Help

Search

Explore the BBC

NEWS

▶ Watch ONE-MINUTE WORLD NEWS

Page last updated at 14:12 GMT, Monday, 23 February 2009

News Front Page

✉ E-mail this to a friend   🖨 Printable version

Workers 'stealing company data'

Africa

By Maggie Shiels

Americas

Technology reporter, BBC News, Silicon Valley

Asia-Pacific

Six out of every 10 employees stole company data when they left their job last year, said a study of US workers.

Europe

Middle East

South Asia

The survey, conducted by the Ponemon Institute, said that so-called malicious insiders use the information to get a new job, start their own business or for revenge.

UK

Business

Health

Science & Environment

Technology

Entertainment

Also in the news

"They are making these judgements based out of fear and anxiety," the Institute's Mike Spinney told BBC News.

Video and Audio

Have Your Say

"People are worried about their jobs and want to hedge their bets,"
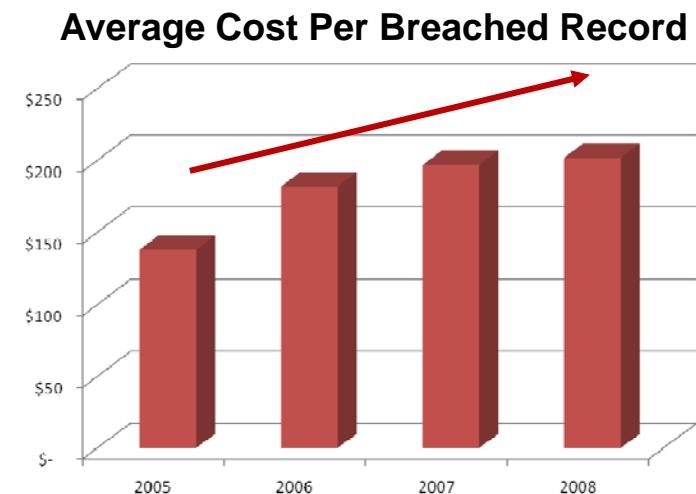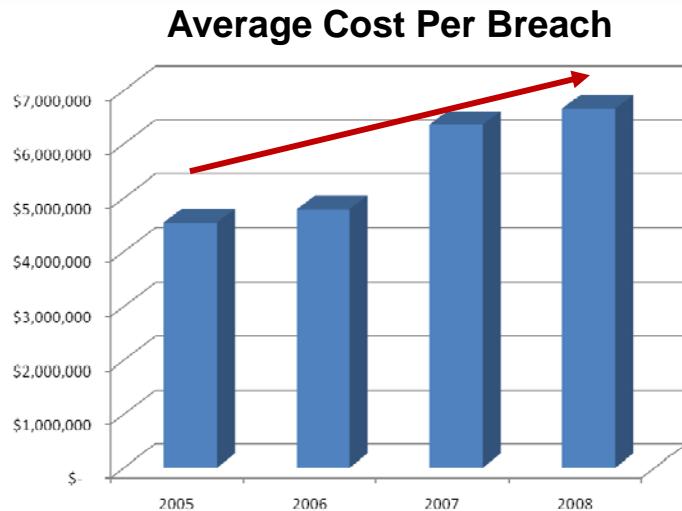
The study said companies fail to take proper steps to stop data theft

SEE ALSO

▸ Malicious insider attacks to rise
   11 Feb 09 | Technology

▸ Thousands hit by breaches of data
   12 Mar 08 | Scotland

▸ Why we need hackers
   15 Nov 02 | Technology

▸ Hi-tech crime: A glossary
   05 Oct 06 | UK

▸ When financial data goes missing
   26 Aug 08 | Business

▸ Extent of data losses is revealed
   19 Aug 08 | UK Politics

▸ Tracking down hi-tech crime
   08 Oct 06 | Technology

▸ Cheese beats crackers

Cost of Data Breaches

Average Cost Per Breach

Breach Costs Break Down

Detection & Escalation 6%

Notification 14%

Ex-post Response 26%

Lost Business 54%

Average Cost Per Breached Record
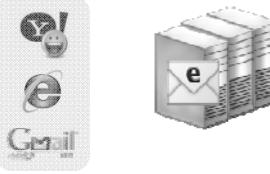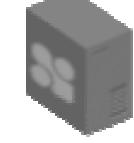
➔ **Tangible financial impact**

➔ **Long-term damage to brand equity**

➔ **Total cost per breach is increasing**

➔ **44 US States have notification laws**

➔ **EU & Australia data privacy policies**

➔ **MAS IBTRM Guidelines**

5

Source: Ponemon Institute 2008 Annual Study on Cost of a Data Breach
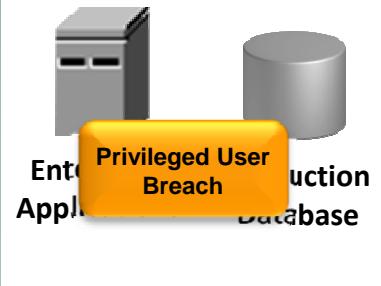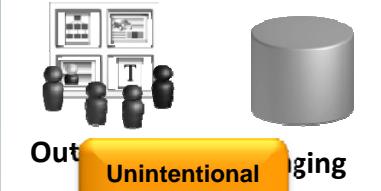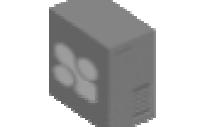
RSA
The Security Division of EMC
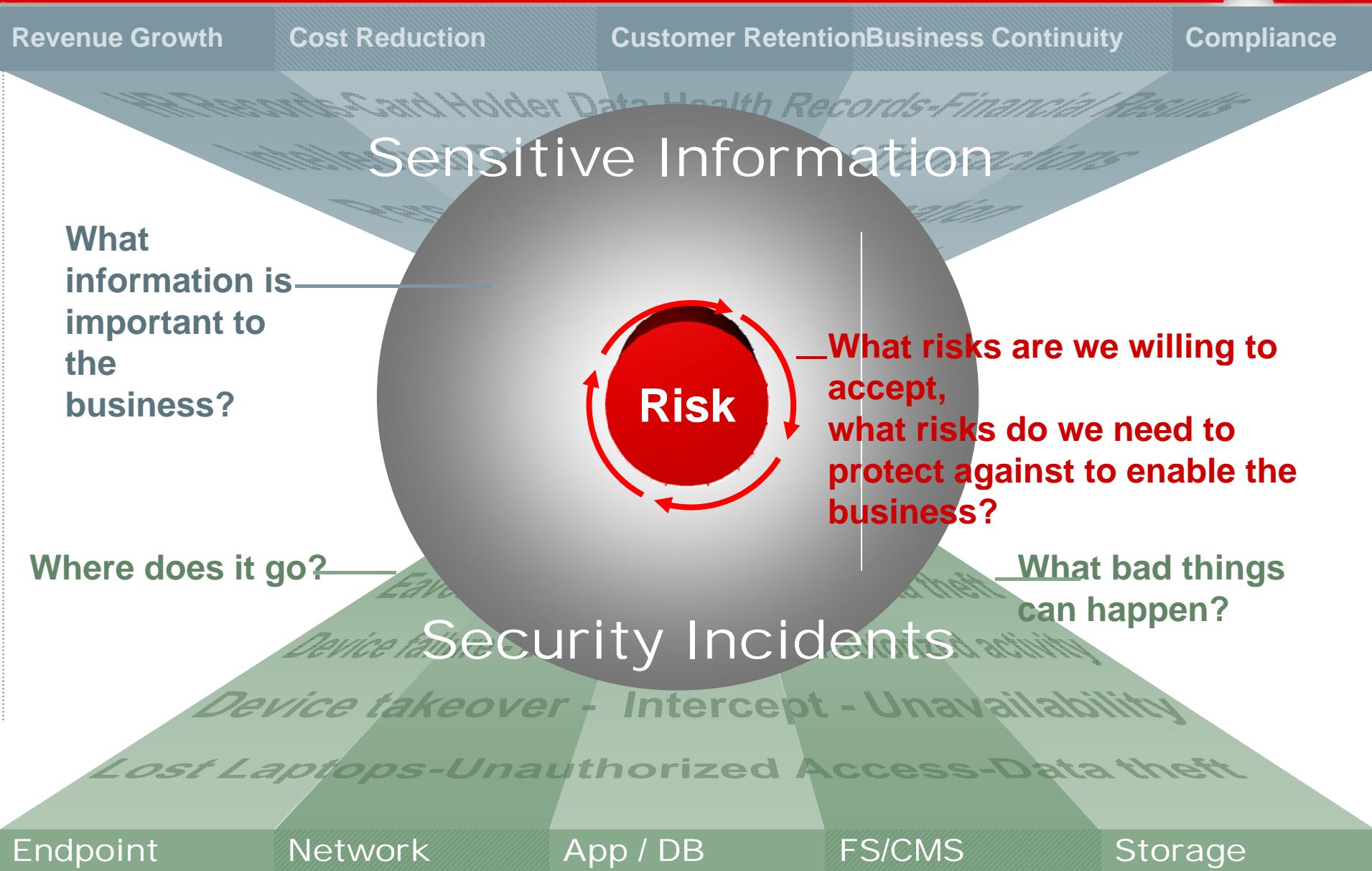
Why is Information Security So Difficult?

Endpoint	Network/E-mail	Apps/DB	FS/CMS	Storage

Endpoint	Network/E-mail	Apps/DB	FS/CMS	Storage

We Are Exposed At Every Point
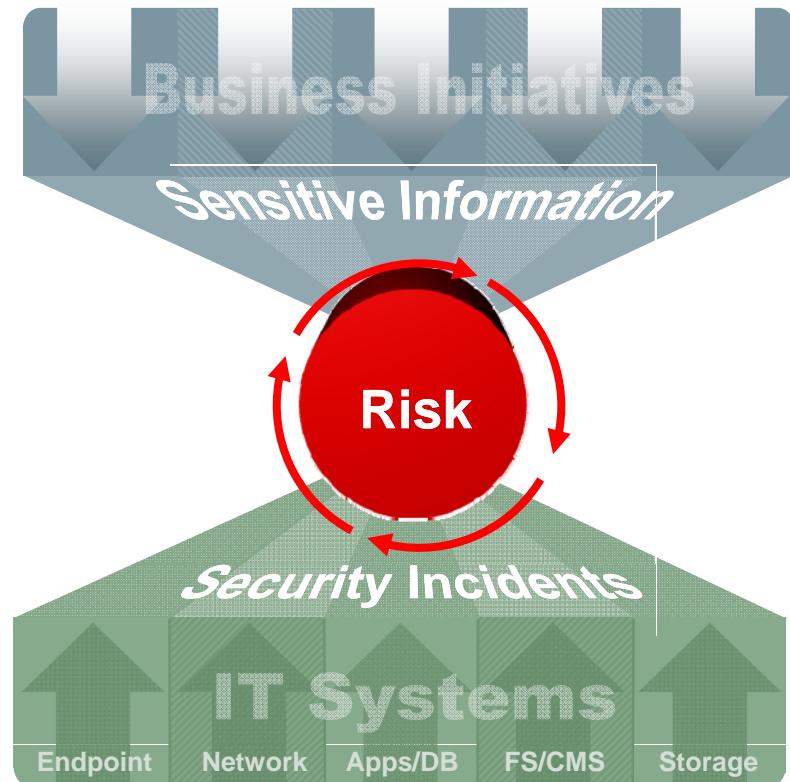
Endpoint	Network/E-mail	Apps/DB	FS/CMS	Storage

Endpoint

Endpoint theft/loss

Endpoint Leak via print/copy

IP Sent to non trusted user

Network/E-mail

LAN

Network Leak Email-IM-HTTP-FTP-etc.

WAN

VPN

E-mail leak or packets sniffed in transit

Public Infrastructure Access Hack

Apps/DB

Ente... ...uction Appl... ...Database

Privileged User Breach

Bu... ...plica Ar...

App, DB or Encryption Key Hack

Out... ...ging

Unintentional Distribution

FS/CMS

Privileged User Breach

File Server / CMS Hack

SharePoint and other ...Systems

(Semi) Trusted User Misuse

Storage

Disk A... ...p Tape

Tapes lost or stolen

Disk Arrays

Backup System

Disk Arrays Backup Disk

Discarded disk exploited

Endpoint	Network/E-mail	Apps/DB	FS/CMS	Storage

Risk Aligns Security Investments to the Business

Revenue Growth	Cost Reduction	Customer Retention	Business Continuity	Compliance

Sensitive Information

Records-Card Holder Data-Health Records-Financial Results

What information is important to the business?

Risk

What risks are we willing to accept, what risks do we need to protect against to enable the business?

Where does it go?

What bad things can happen?

Security Incidents

Eavesdrop
Device takeover - activity
Device takeover - Intercept - Unavailability
Lost Laptops-Unauthorized Access-Data theft

Endpoint	Network	App / DB	FS/CMS	Storage

Information Risk Management
a strategy for protecting your most critical assets

Information-centric

Clarifies business context and reveals potential vulnerabilities

Risk-based

Establishes a clear priority for making security investments

Repeatable

Based on foundation of broadly applicable best practices and standard frameworks

**Reveals where to invest, why to invest, and how security investments map to critical business objectives**

RSA®
The Security Division of EMC
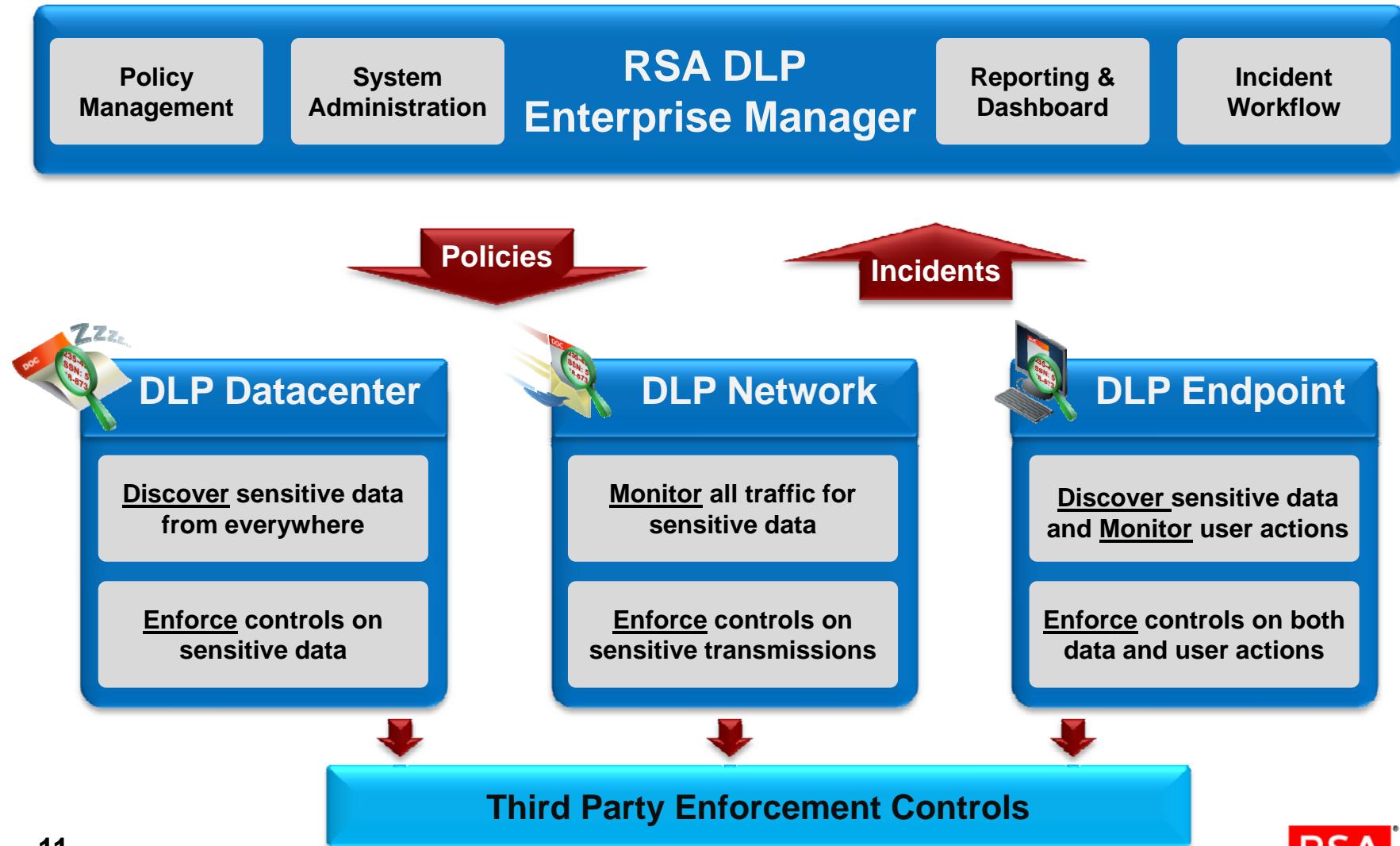
RSA Data Loss Prevention

Data Breaches Overview
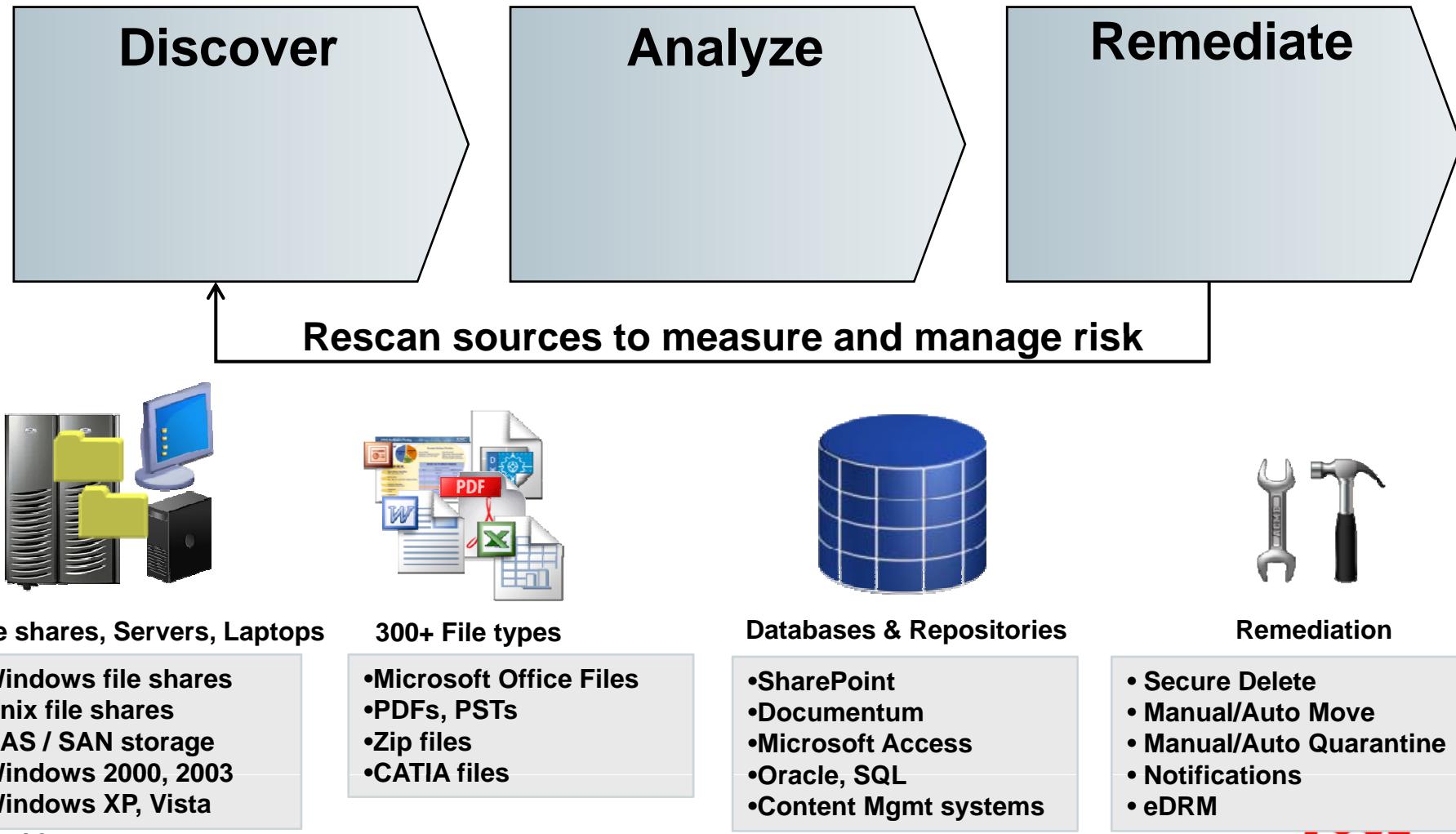
RSA DLP Solution

Five Critical Factors

RSA Data Loss Prevention Suite

Policy Management	System Administration	**RSA DLP Enterprise Manager**	Reporting & Dashboard	Incident Workflow

Policies ⬇

Incidents ⬆

DLP Datacenter

Discover sensitive data from everywhere

Enforce controls on sensitive data

DLP Network

Monitor all traffic for sensitive data

Enforce controls on sensitive transmissions

DLP Endpoint

Discover sensitive data and **Monitor** user actions

Enforce controls on both data and user actions

Third Party Enforcement Controls

11

RSA
The Security Division of EMC

Reducing Your Sources of Risk: Data at Rest

Discover → **Analyze** → **Remediate**

Rescan sources to measure and manage risk

File shares, Servers, Laptops

- Windows file shares
- Unix file shares
- NAS / SAN storage
- Windows 2000, 2003
- Windows XP, Vista

300+ File types

- Microsoft Office Files
- PDFs, PSTs
- Zip files
- CATIA files

Databases & Repositories

- SharePoint
- Documentum
- Microsoft Access
- Oracle, SQL
- Content Mgmt systems

Remediation

- Secure Delete
- Manual/Auto Move
- Manual/Auto Quarantine
- Notifications
- eDRM

12

RSA
The Security Division of EMC

Protecting Data in the Network: Data in Motion

Monitor **Analyze** **Enforce**
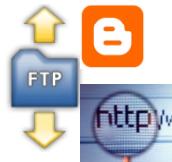
Email

- •SMTP email
- •Exchange, Lotus, etc.
- •Webmail
- •Text and attachments

Instant Messages

- •Yahoo IM
- •MSN Messenger
- •AOL Messenger

Web Traffic

- •FTP
- •HTTP
- •HTTPS
- •TCP/IP

Remediation

- •Audit
- •Block
- •Encrypt
- •Log

RSA®
The Security Division of EMC
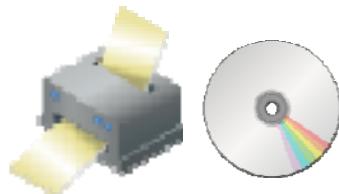
Protecting Data at the Endpoint: Data in Use

Monitor → **Analyze** → **Enforce**

Print & Burn
- Local printers
- Network printers
- Burn to CDs/DVDs

USB
- External hard drives
- Memory sticks
- Removable media

Copy and Save As
- Copy to Network shares
- Copy to external drives
- Save As to external drives

Actions & Controls
- Allow
- Justify
- Block
- Audit & Log

14

RSA
The Security Division of EMC

How Can DLP Solutions Reduce Risk?

Endpoint	Network	Apps/DB	FS/CMS	Storage

People
- **Discover unsafe user behavior and educate employees on security policies**

Processes
- **Identify and fix broken business processes**

Technology
- **Leverage technology controls more effectively to secure data**
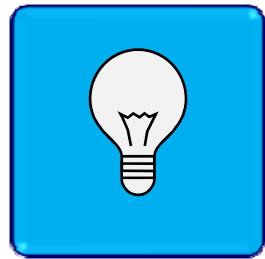
RSA Data Loss Prevention

Data Breaches Overview

RSA DLP Solution

Five Critical Factors

Top 5 Critical Factors for DLP
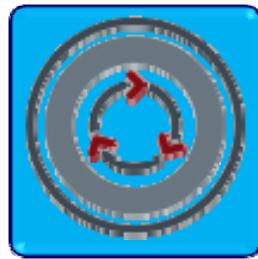
Policy & Classification

More policies and better policies for classification and risk mitigation

Identity Aware

Identity awareness for classification, controls and remediation

Incident Workflow

Consolidated alerts with the right information to the right people for the right actions

Enterprise Scalability

Scan more data faster with lesser hardware and resources

Built-In vs. Bolt-On

Common policies across the infrastructure - Microsoft and Cisco

RSA ®
The Security Division of EMC

Policy & Classification

More policies and better policies for classification and risk mitigation

- Unified policy framework

- Best of breed classification

- 150+ built in policy templates

- Information Policy and Classification team

- Higher accuracy

Identity Awareness

Identity awareness for classification, controls and remediation

- Identity-based Policy
    E.g. Group x can send data y out

- Identity-based notification
    E.g. Notify the persons manager

- Identity-based control
    E.g. Lock this data so only group x can open

- Integration with Microsoft Active Directory

RSA
The Security Division of EMC

Incident Workflow

**Consolidated alerts with the right information to the right people for the right actions**
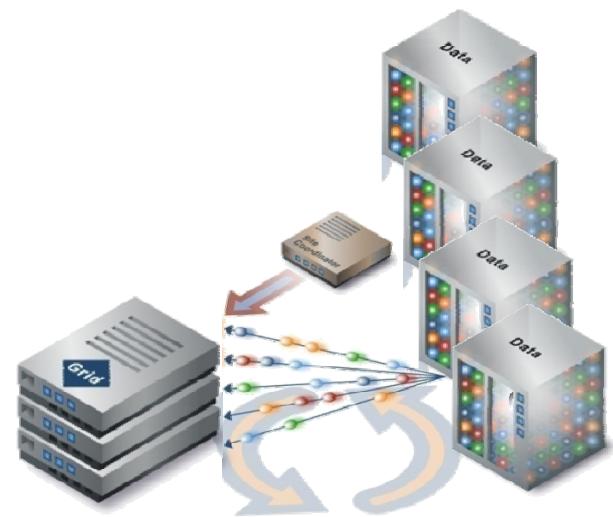
- Intelligent correlation of events into incidents

- Right alerts to the right people in the right order

- Intuitive workflow to remediate violations

- Scheduled reports sent to subscribers automatically

- Integration with RSA enVision to simplify security operations

RSA
The Security Division of EMC

Enterprise Scalability

E ✓ **Scan more data faster with lesser hardware and resources**

- Support distributed deployments

- Scale to 100's of thousands of users

- Unique Grid Scanning technology

- Scan large amounts of data faster and cheaper

RSA
The Security Division of EMC

Built-in Vs. Bolt-on

Common policies across the infrastructure –

Microsoft and Cisco

- Leverage your existing infrastructure

- Microsoft: Integration with Microsoft RMS and will also integrate RSA DLP data classification engine and policies into Microsoft infrastructure

- Cisco: Integration with IronPort

Microsoft®

CISCO

RSA®
The Security Division of EMC

RSA DLP Suite integration with Microsoft AD RMS

RSA
The Security Division of EMC

EMC²
where information lives®

Home > About RSA > News & Events

Press Releases

Thursday, December 04, 2008

Microsoft and EMC'S RSA Security Division Team Up to Help Customers Secure Sensitive Data

Companies Expand Their Strategic Alliance to Advance a New Approach to Information Protection and Data Loss Prevention

Hopkinton, Ma and Redmond, Wa

— Building on a long-standing, multi-faceted alliance, EMC and Microsoft Corp. today announced they have expanded their technology partnership to help companies better protect sensitive information and share it in a more secure manner. The companies will be working together with a built-in "systems" approach that helps protect information throughout the infrastructure based on content, context and identity.
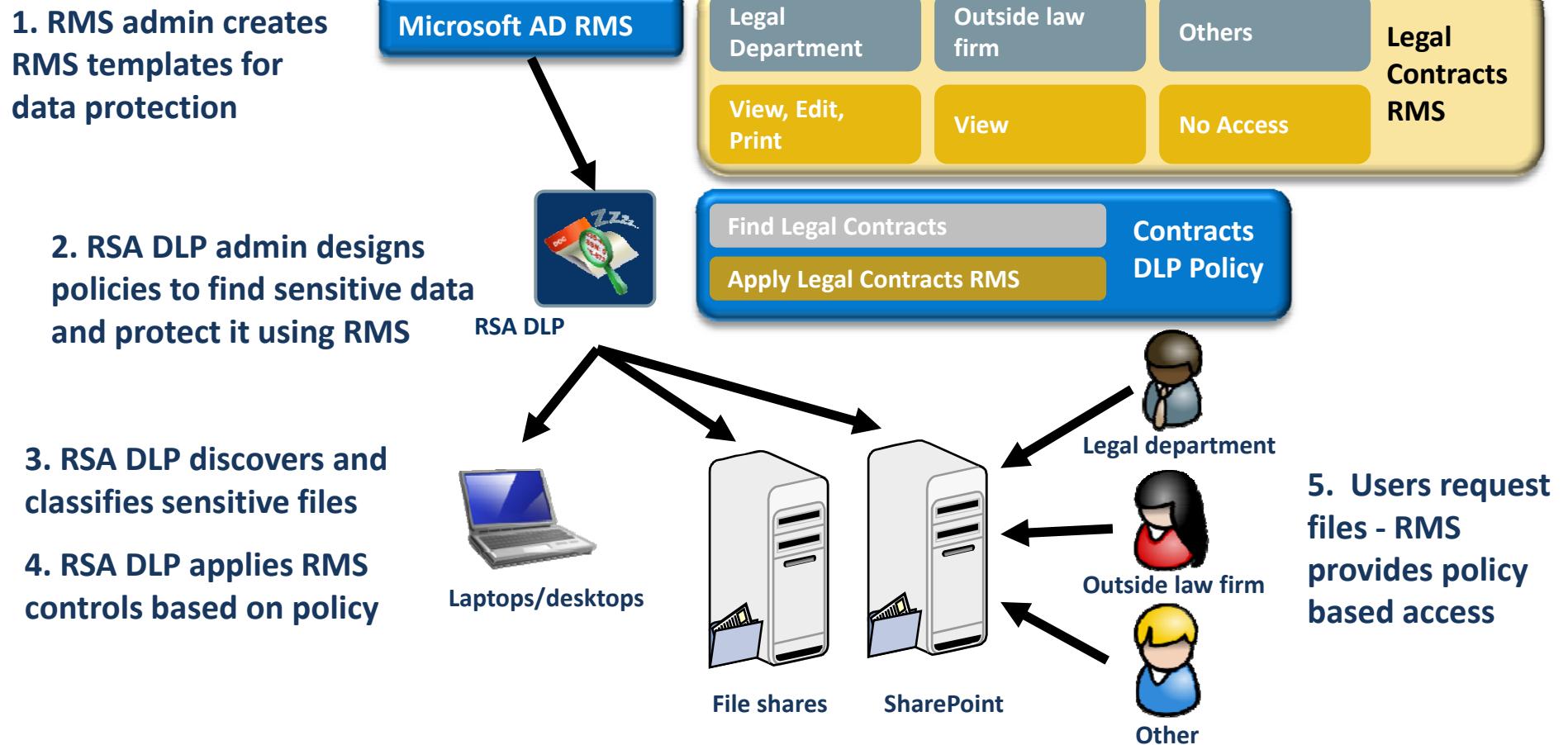
The partnership will take advantage of resources and technology from Microsoft and RSA, The Security Division of EMC. Microsoft will build the RSA® Data Loss Prevention (DLP) classification technology into the Microsoft platform and future information protection products. The resulting collaboration is designed to enable organizations to centrally define information security policy, automatically identify and classify sensitive data virtually

Rights Management Services Overview

Persistent Protection

Encryption **+** Policy:
- **Access Permissions**
- **Use Right Permissions**
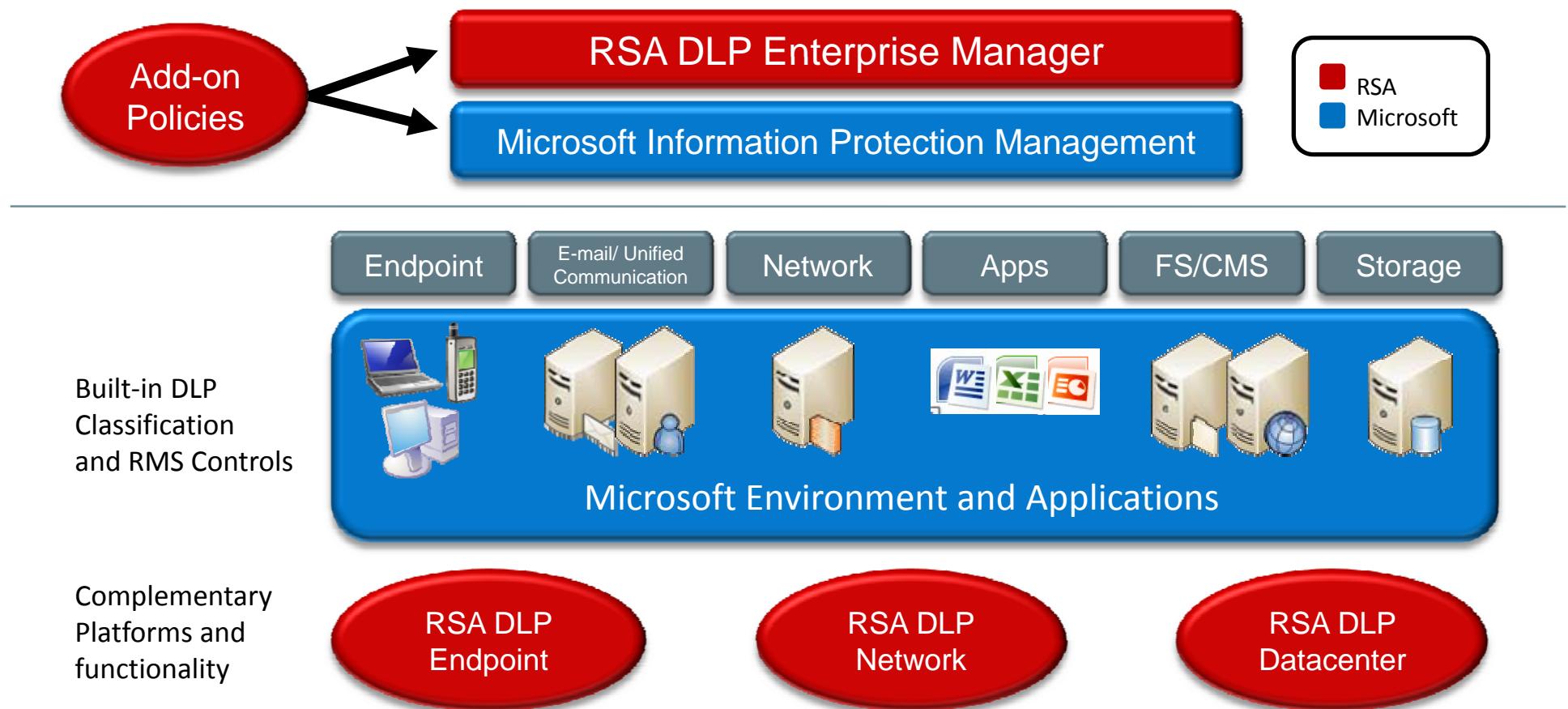
- **RMS provides identity-based protection for sensitive data**
  - Controls access to information across the information lifecycle
  - Allows only authorized access based on trusted identity – works online and offline, inside and outside the firewall
  - Secures transmission and storage of sensitive information wherever it goes – policies embedded into the content; documents encrypted
  - Embeds digital usage policies (print, view, edit, expiration etc.) in to the content to help prevent misuse after delivery

RSA DLP Suite integration with Microsoft AD RMS

1. RMS admin creates RMS templates for data protection

Microsoft AD RMS

Legal Department	Outside law firm	Others	**Legal Contracts RMS**
View, Edit, Print	View	No Access	

2. RSA DLP admin designs policies to find sensitive data and protect it using RMS

RSA DLP

Find Legal Contracts	**Contracts DLP Policy**
Apply Legal Contracts RMS	

3. RSA DLP discovers and classifies sensitive files

4. RSA DLP applies RMS controls based on policy

Laptops/desktops

File shares   SharePoint

Legal department

Outside law firm

Other

5. Users request files - RMS provides policy based access

- **Automate the application of AD RMS protection based on sensitive information identified by RSA DLP Datacenter and DLP Endpoint Discover**
- **Leverage AD Groups with DLP Network and Endpoint Enforce for identity or group aware data loss prevention**

Long term – Microsoft and RSA Building Information Protection into Infrastructure

Add-on Policies

RSA DLP Enterprise Manager

Microsoft Information Protection Management

RSA
Microsoft

Endpoint | E-mail/ Unified Communication | Network | Apps | FS/CMS | Storage

Built-in DLP Classification and RMS Controls

Microsoft Environment and Applications

Complementary Platforms and functionality

RSA DLP Endpoint

RSA DLP Network

RSA DLP Datacenter

- Common policies throughout infrastructure
- Built-in approach to protect data based on content, context, identity

RSA
The Security Division of EMC

RSA and Cisco Partner to Better Secure Data

RSA
The Security Division of EMC

EMC²
where information lives®

Search [   ] **Go**

Press Releases

Wednesday, June 24, 2009

RSA Embeds Data Loss Prevention Technology and Policies Into Cisco Ironport® Email Security Solutions
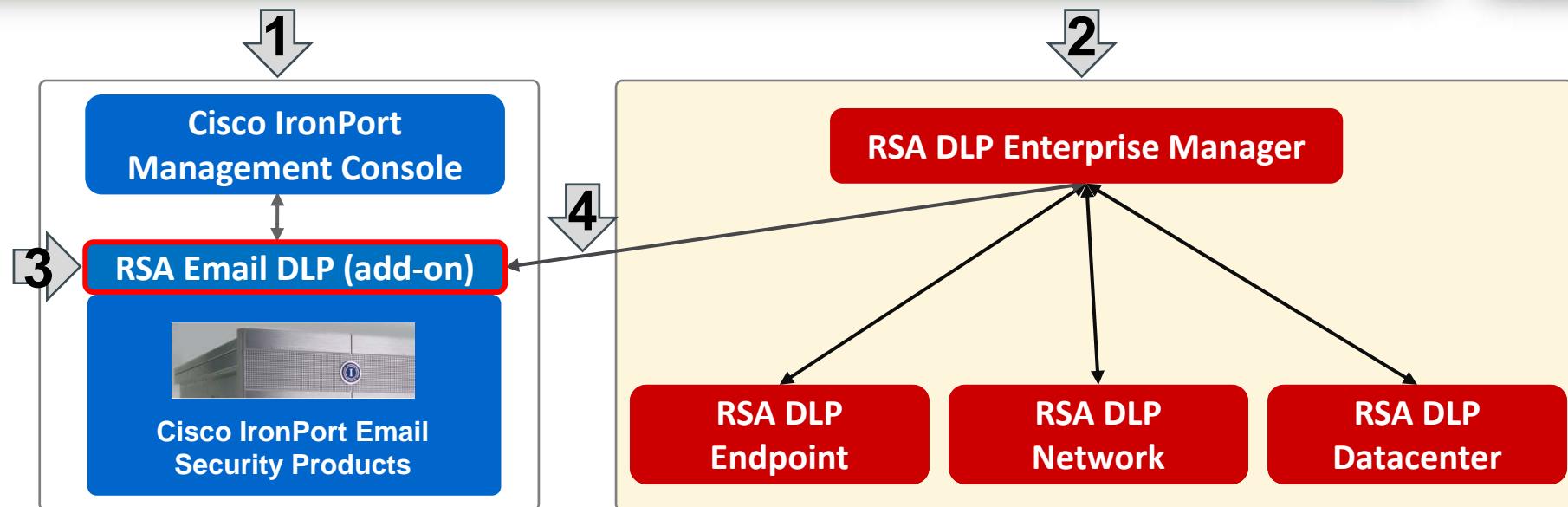
EMC's Security Division and Cisco IronPort Provide Built-in Data Loss Prevention to Help Secure IT Infrastructure

Bedford, Ma

— RSA, The Security Division of EMC (NYSE: EMC), today announced that it has partnered with Cisco to embed data classification technology and policies from the RSA® Data Loss Prevention Suite into Cisco's industry-leading Cisco IronPort® email security solutions. RSA's DLP technology will be fully integrated into Cisco IronPort's email security platform as a comprehensive subscription software service for helping to prevent the loss of data in motion over email. The combined solution, to be offered as RSA Email DLP for Cisco IronPort, provides accurate and easy-to-use content classification designed to discover and protect sensitive data before it leaves the enterprise through email.

The integrated RSA Email DLP solution is engineered to include a wide selection of pre-defined out-of-the-box policies maintained and updated by RSA's Information Policy and

RSA and Cisco Partner to Better Secure Data

1

2

Cisco IronPort Management Console

RSA Email DLP (add-on)

3

Cisco IronPort Email Security Products

4

RSA DLP Enterprise Manager

RSA DLP Endpoint

RSA DLP Network

RSA DLP Datacenter

Prevent loss of sensitive data through email with industry best accuracy

Expand to DLP for datacenter, endpoints and web through RSA DLP Enterprise Manager, leveraging policy and classification framework

RSA Cisco

1. **Cisco IronPort Email Security Solutions**
2. **RSA Data Loss Prevention Suite**
3. **Cisco IronPort RSA Email DLP**
4. **Expandability of DLP to datacenter, network and endpoints**

RSA
The Security Division of EMC

Thank You

Kelvin Wee CISA, CISM, CISSP
Principal Consultant (DLP Specialist) – APJ
kelvin.wee@rsa.com