A Complimentary Webinar Series:

Building a Data Privacy Compliant Records Management Program

Data Privacy Compliance—
A Deep Dive Into Understanding the Requirements

November 2, 2011

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Welcome!

- **Housekeeping…**
  - Control panel on the right side of your screen.
  - Audio
    - Telephone
    - VoIP
  - Submit “Questions” in the pane on the control panel and we will address questions at the end of the session.
  - Minimize pane during presentation – Click double arrows icon top-left of the control panel.
  - **Need help? Call 800-263-6317**

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Introductions

PIVOT GROUP
Armed with Information Security Knowledge

Pivot Group

Independent Audit, Assessment and Compliance Firm providing exclusively Data Privacy and Protection Services.

CINTAS
DOCUMENT MANAGEMENT

Cintas Document Management

Cintas was the first North American AAA NAID Certified and PCI-DSS Compliant Provider. Cintas has service locations throughout the entire US, parts of Canada and Europe and offers document imaging, records storage and secure shredding that keeps your business, employee and customer data protected.

Introductions - Presenter

Jim Soenksen – CEO

- 20 years of experience in the information security and technology industries.
- As a CPA was also an internal auditor for a fortune 100 company for 7 years.
- Conveys the knowledge and conviction it takes to fight cyber crime
- Offers a realistic view of today's security issues and remedies for businesses.
- Blends business goals with technology, training, policies, and improved processes to provide the appropriate security program, technology controls, and regulatory compliance for each individual companies needs.

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Today's Learning Objectives

- Federal Privacy Requirements including GLBA, HIPAA/HITECH ACT, PCI, and Red Flags
- State Data Privacy Regulatory Requirements
- Impact of Noncompliance
- Technologies that can help manage and monitor data privacy and security.
- How to perform a "health check" of your incident response program.

PIVOT GROUP
Armed with Information Security Knowledge

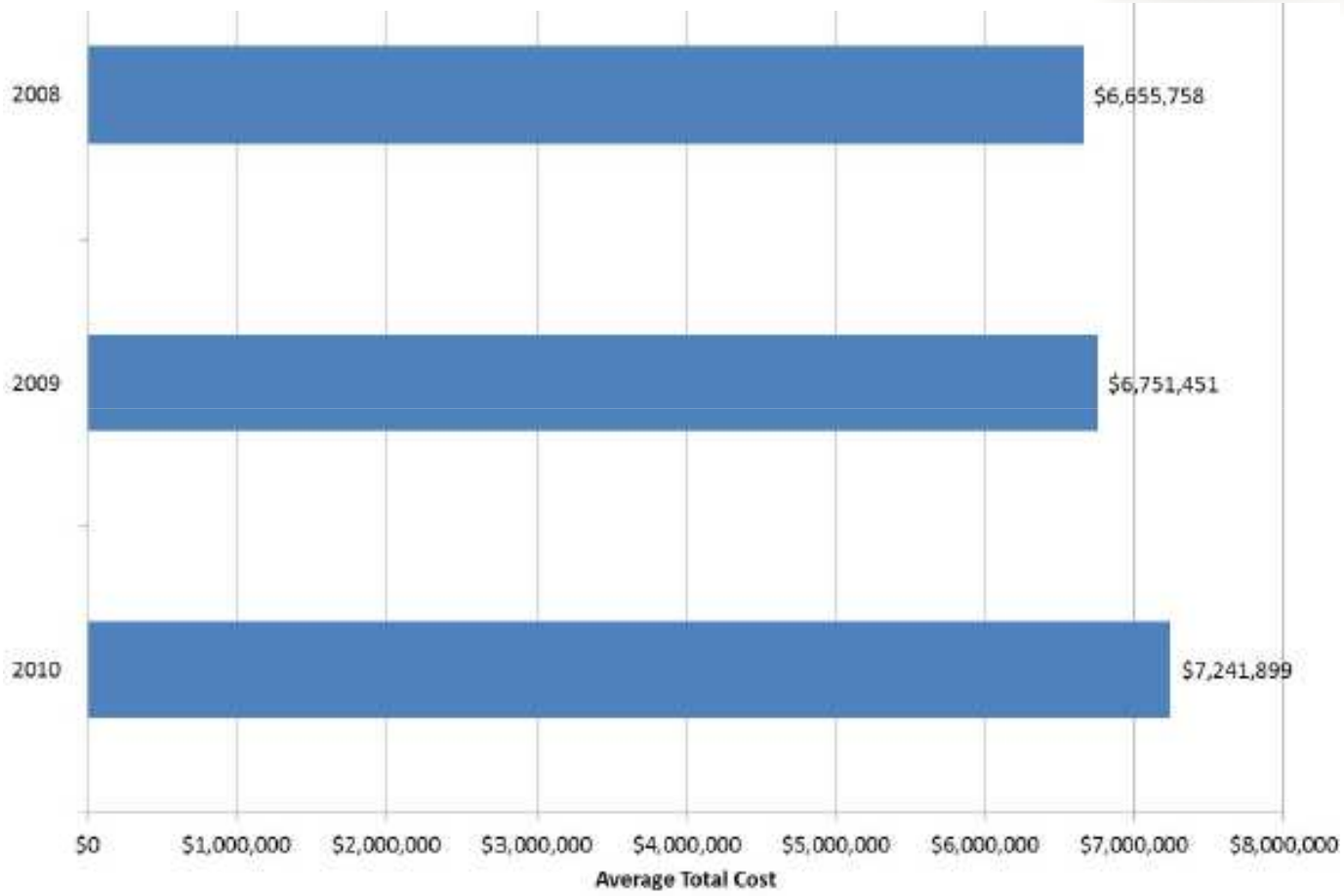
CINTAS
DOCUMENT MANAGEMENT

Recent High Profile Incidents

- **Epsilon**
  - Phishing Attack
  - Email
  - Vendor Management
- **State of Texas- 3.5 Million Records**
  - Policy Enforcement
  - Database Security
  - Data Management
- **RSA Secure ID**
  - Data Base/Key Fob Breach
  - Social Engineering- Email, Excel
  - Zero Day Adobe Flash Vulnerability
- **Wiki-Leaks**
  - Data Management and Protection

Ponemon 2010 Data Breach Cost Study

Average organizational cost of data breach, 2008-2010

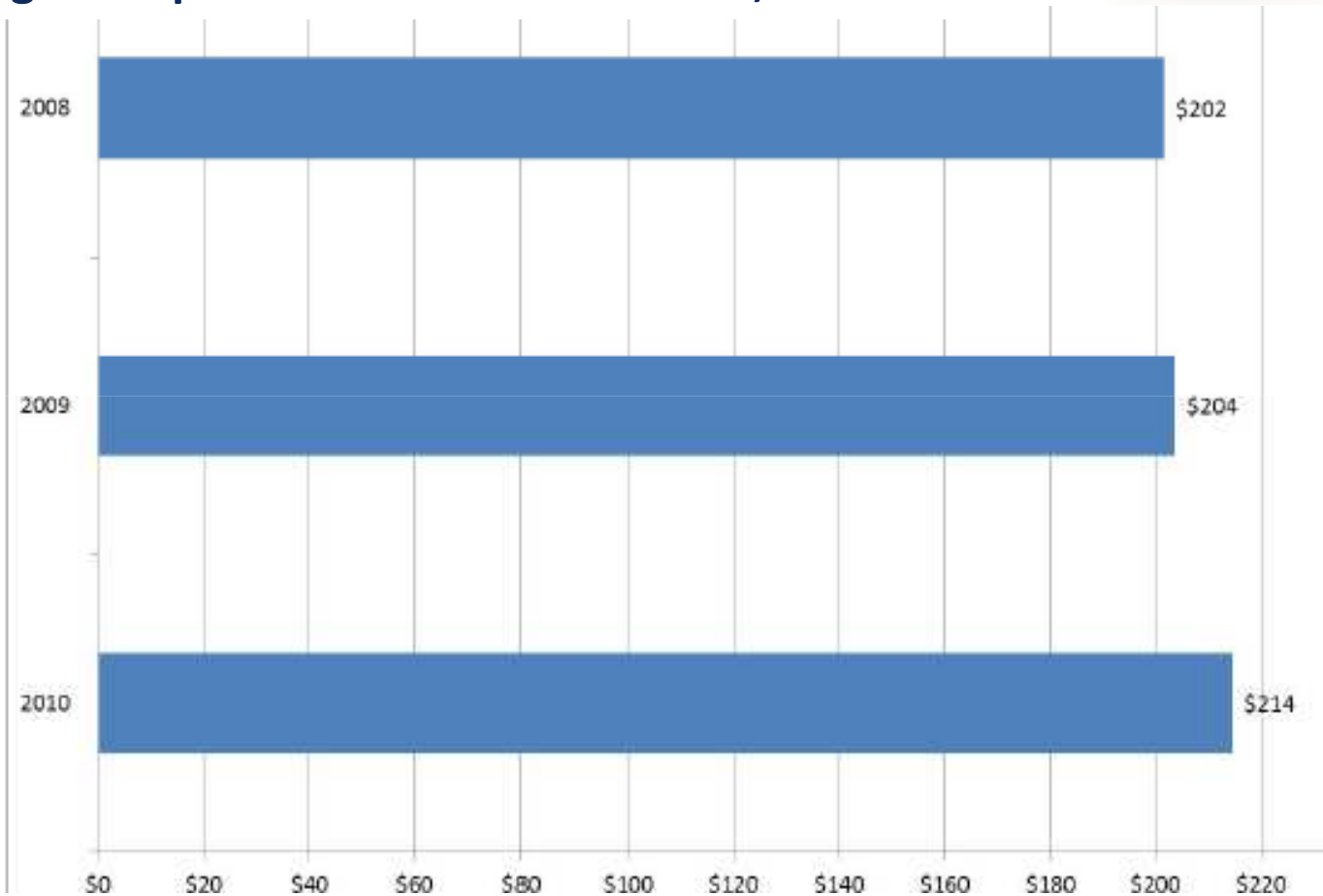


PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Ponemon 2010 Data Breach Cost Study

Average cost per record of a data breach, 2008-2010



PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

What Data to Protect ????

To understand the scope of privacy/security laws, you must address:

- **Data at Rest**
  - Information sitting on your network, office and/or storage
- **Data in Use**
  - Data that is being worked on in the office, at home, on a mobile device (Blackberry, iPhone), in a public location, at a service providers
- **Data in Transit**
  - Any data moving from point A to point B via email, extranets, intranets, service providers, via FedEx, USPS, courrier, document management, etc.

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Data Privacy &Protection (DP&P) Vocabulary

- **Personally Identifiable Information (PII)**
  - Information that can be used to identify an individual or can be used with other sources to identify an individual (SSN, name, address, tax ID, etc.)
- **Protected Health Information (PHI)**
  - Data that contains information relating to a medical condition and also contains PII. (ePHI: electronic PHI)
- **Payment Card Industry (PCI)**
  - Data that contains credit/debit card information
- **Financial Information**
  - Credit card numbers, banking information, investment account numbers - includes information in any form, paper or electronic
- **Business Associate**
  - Anyone with whom you are sharing protected information

Primary Industries and Data Affected

- Financial Services
- Healthcare
- Retail
- Law Firms
- Federal, State, & Local Government
- PII Data
- PHI Data
- PCI Data
- State Resident's Data
- Canadian or European Resident's Data
- Intellectual Property
- Electronic Discovery

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

111th & 112th Congress DP&P Bills

111th Congress

- 21 Bills/Resolutions Introduced
- 2 Passed
- 19 Pending

112th Congress

- 18 Bills/Resolutions Introduced

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Current Data Privacy Regulations

Regulatory Compliance

- GLBA/NCUA Reg.748
- Important to viability of institution to securely safeguard member data
- Customers require that the institution comply with their applicable regulators
- Institutions have a tested Incident Response Program

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Current Data Privacy Regulations (cont.)

Data Security Breach Notification Laws

- 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands

  (Except Alabama, Kentucky, New Mexico and South Dakota)

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Current Data Privacy Regulations (cont.)

Other Applicable Laws

- **PCI** – must protect credit card numbers, Mask PAN (*primary account number*) when displayed
  - First 6 and last 4 digits are the maximum number of digits to be displayed
- **HIPAA/HiTECH Act**
  - Security controls, how long retain data, and destruction procedures
  - Privacy of medical information
- **Fair Credit Reporting Act (FCRA) and Fair Accurate Credit Transactions Act (FACTA)**
  - Must take reasonable measures to dispose of sensitive information from credit reports and background checks
- **Red Flag Rules** – written identity theft prevention program
- **Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)**
  - Covers all industries and protects the collection, usage and disclosure of personal information

State Regulatory Requirements

Massachusetts - 201CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth

- Development of a written comprehensive information security plan that includes security policies, monitoring, security breach notifications, and employee training
- Must encrypt PII on/in:
- Laptops
- Removable media devices
- E-mail messages

Nevada Revised Statutes (NRS) 597.970

- Mandates encryption for the transmission of Nevada resident PII through electronic means other than via a fax or on an internal secured system

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Parties to Notify (Varies by State)

- Affected State Residents
- Owner or Licensee of Information
- Credit Reporting Agencies
  (Dependent upon number of persons affected)
- Attorney(s) General
- Secret Service (D.C. only)
- Office of Consumer Protection

Impact of Non-Compliance

- **Stiff Penalties**
  - Ranging from $250 - $500 per person to a maximum of $750,000 per incident in some states
- **Damage to Brand**
  - Negative Press
  - Image tarnished
  - Lack of trust

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Incident Response Health Check

- Ensure Sensitive Data is Defined, Classified, & Located
- Definition of a Breach
- Establish Internal Escalation & Reporting Procedures
- Review Vendors IR
- Establish IR Team
- Establish External Reporting Procedures
- Test & Adjust IR Regularly

PIVOTGROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Federal Rules of Civil Procedures

- Electronically-stored information (ESI) is discoverable. May be used as evidence — for or against your company.
- Business record email, social media posts & other ESI must be saved, stored, & supplied ***swiftly*** and in a ***legally compliant*** fashion.
- To be accepted as legal evidence, email, social media content, and other ESI must be preserved and produced in a trustworthy, tamperproof, legally-compliant manner.
- OK to routinely purge ESI not relevant to litigation or pending cases (or otherwise required by law/regulator).
- You must anticipate likelihood of ***future*** litigation

Obstacles

- Lack of Ownership
- No Metrics
- No Risk Management
- No Education

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Success Factors

- Don’t Ignore…Be Informed!
- Current Policies
- Effective Monitoring & Reporting
- Easy to Use
- When something happens…know what to do!

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Ponemon 2010 Data Breach Cost Study

Preventative measures implemented as a result of a data breach

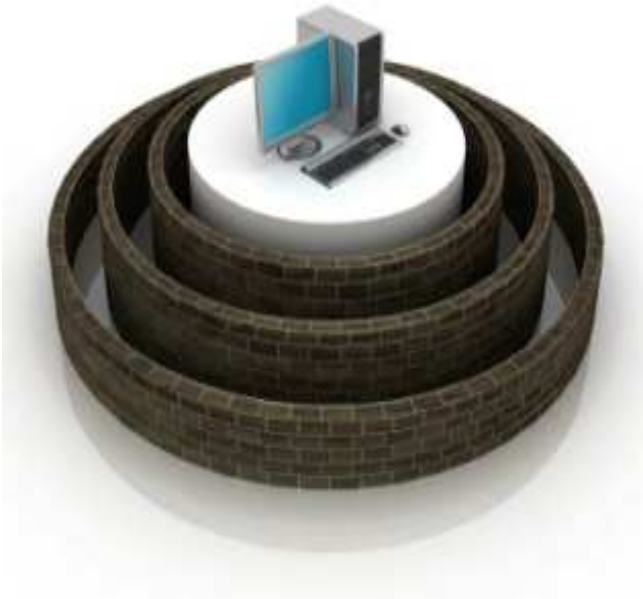
Preventative Measure	2010	2009	2008
Training and awareness programs	63%	67%	53%
Expanded use of encryption	61%	58%	44%
Additional manual procedures and controls	54%	58%	49%
Identity and access management solutions	52%	49%	37%
Data loss prevention (DLP) solutions	43%	42%	26%
Other system control practices	43%	40%	40%
Endpoint security solutions	41%	36%	19%
Security certification or audit	29%	33%	30%
Strengthening of perimeter controls	22%	20%	16%
Security event management systems	21%	22%	21%

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Technologies that Help

- Data Discovery
- AntiVirus/AntiSpam
- Access Control
- Patch Management
- Vulnerability Management
- IDS/IPS
- Encryption
- DLP
- GRC



PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Locating Critical Data

“How do we know we have a problem if we can’t see it?”

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Data Discovery Results

1. Audit

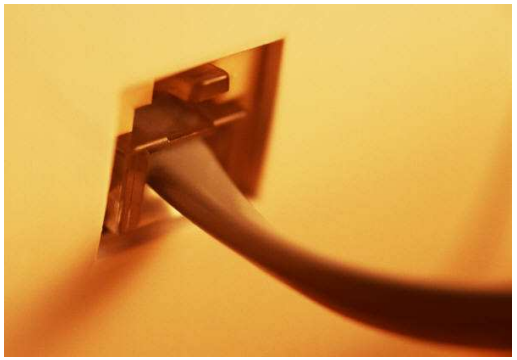
- System
- Data
- Processes

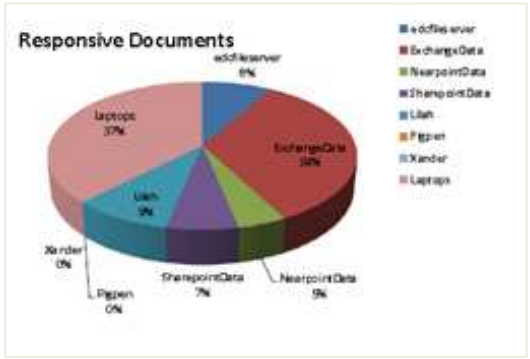
2. Analysis

- Process overview
- Data discovery
- Behavioral observations

3. Actions

- Plan for today
- Prevention for tomorrow





PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Regular Monitoring and Audits

“How do we avoid problems in the future?”

- Regular Audits and Follow-up
- Policy Enforcement
- Changing Processes/Behaviors

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

New Technology Deployment

- Layered Security
- Monitoring and Logging
- Encryption
- VoIP/Wireless/Bluetooth
- Mobile Applications/Devices
- Social Media
- SaaS
- Virtual Computing
- Cloud Computing

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Technology Deployment Checklist

- ✓ Identify Critical Data
- ✓ Identify Critical Data Access, Storage, Retention, Destruction
- ✓ Identify OTHER Critical System Access
- ✓ Determine Data & System Risk
- ✓ Determine Risk Controls
- ✓ Implement and Test in Pre-Production Environment
- ✓ Protect Test Data and Environment
- ✓ Controlled Roll Out
- ✓ Include in Regular PII Risk Assessments

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Today's Take Aways

- Threats are Increasing
- Data Breach Costs are Increasing
- Regulatory Compliance is Increasing
- New Technologies are in Demand
- Implement a Records Management Program
- Implement & Monitor Risk Based Best Practices
- Implement into Your ERM Framework
- Manage Your Vendors
- Be Prepared for a Data Breach

PIVOT GROUP
Armed with Information Security Knowledge

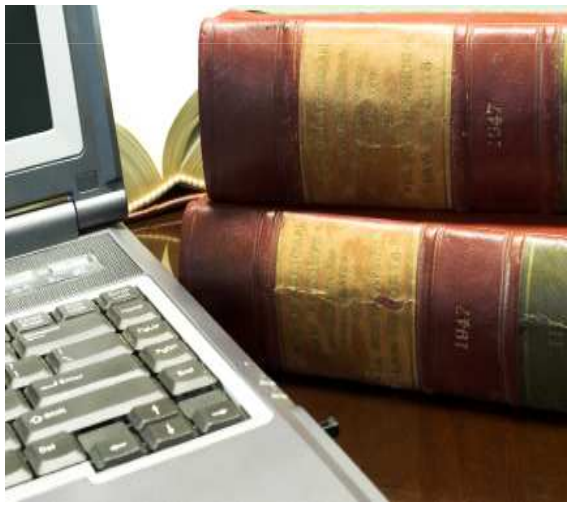
CINTAS
DOCUMENT MANAGEMENT

Helpful Sites

- Fraud Watch
  - http://www.fraudwatchinternational.com/phishing
- FBI
  - http://www.fbi.gov/cyberinvest/escams.htm
- CERT
  - http://www.cert.org/insider_threat/
- Data Loss Data Base
  - http://datalossdb.org/
- APWG
  - http://www.antiphishing.org/
- Dark Reading
  - http://www.darkreading.com/index.jhtml

Reference Resources

- CSO Online
- National Conference of State Legislatures
- ISO 27000
- PCI Security Standards
- Ponemon & PGP *2010 Annual Study: Cost of a Data Breach*
- MER Conference/Sedona Group
- AIIM
- ARMA
- International Threat Resource Center
- Pivot Group Critical Data Check List
- Cintas Records Compliance Guide



PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

November 16 Webinar

Topic: Building an Effective & Compliant Records Management Program

Featured Speaker: Patrick Cunningham, CRM, FAI
Senior Director, Information Governance
Motorola Solutions, Inc

Learning Objectives:

- Records Management Best Practices
- Mitigating Risks Associated with Data Breaches
- Auditing Techniques and Technologies that Overcome Common Hurdles
- RIM Data Privacy Compliance Checklist

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

How to Register

- Webinar E-vites
- Webinar Follow Up E-mail
- www.pivotgroup.com/webinars

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Q&A

For more information contact:

Pivot Group

- Jim Soenksen, CEO
- Call: (888) 722-9010
- Email: jsoenksen@pivotgroup.com
- Visit: www.pivotgroup.com

Cintas

- Call: 1-800-Cintas-1
- Visit: www.cintas.com/documentmanagement

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT