Protecting Company Confidential or Proprietary Information in the Electronic Age

Sandra A. Jeskie

Partner, Duane Morris LLP

Pamela Lehrer

Vice President and General Counsel
Berwind Group

Protected Information

- Trade Secrets
- Personally Identifiable Information
  - Consumers
  - Employees
- Company Proprietary Information

Laws Relating to Personally Identifiable Information ("PII")

- Financial Services
- Health Care
- Education
- Telecommunications
- Children
- Miscellaneous (drivers license, video rental, etc.)

Sarbanes Oxley Act of 2002 “SOX”

- Section 404
  - Establish and maintain adequate “internal controls” for financial reporting, and
  - Assess annually the effectiveness of these controls.

SOX

- Section 404 and its implementing Rules do not expressly require IT security

  BUT, as a practical matter, compliance necessitates adequate IT security

  - requires disclosure of “material weaknesses”

Gramm Leach Bliley ("GLB")

- Establishes obligations for "financial institutions"
  - Banks and lenders,
  - check-cashing businesses,
  - professional tax preparers,
  - mortgage brokers,
  - credit counselors,
  - real estate settlement companies, and
  - retailers that issue credit cards to consumers, etc.

GLB – Safeguards Rule

- Must implement a written information security program
  1. identify and assess the risks to customer information and evaluate effectiveness of current safeguards
  2. Design and implement a safeguards program and establish regular monitoring and testing

GLB - Safeguards Rule

3. Select appropriate service providers and contract with them to implement safeguards

4. Evaluate and adjust the program in light of relevant circumstances including:
   - changes in business or
   - the results of testing and monitoring

GLB

When a security breach occurs:

- Implement an incident response plan with the following procedures (at a minimum):
  - assess the nature and scope of the incident
  - appropriate notification
  - steps to contain and control the incident

HIPAA

- Impacts all organizations within the healthcare industry, and those which process or use healthcare information, such as:
  - private health plans,
  - healthcare providers, and
  - healthcare clearinghouses

HIPAA

- “PHI” is information that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual.

45 C.F.R. 160.103.

DuaneMorris

HIPAA – Security Rule

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

ITAR

- International Traffic in Arms Regulation
  - Regulates the export and import of defense-related articles and services
  - Prohibits disclosure of certain information to non-US citizens, including employees and non-US companies
  - Requires segregation and regulation of information

Privacy Laws

- No privacy authority whose sole job is enforcement of privacy laws

Federal Trade Commission ("FTC")

- Enforces laws that prohibit business practices that are anti-competitive, deceptive, or unfair to consumers

- Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."

  15 U.S.C. Sec 45 (a)(1)

DuaneMorris

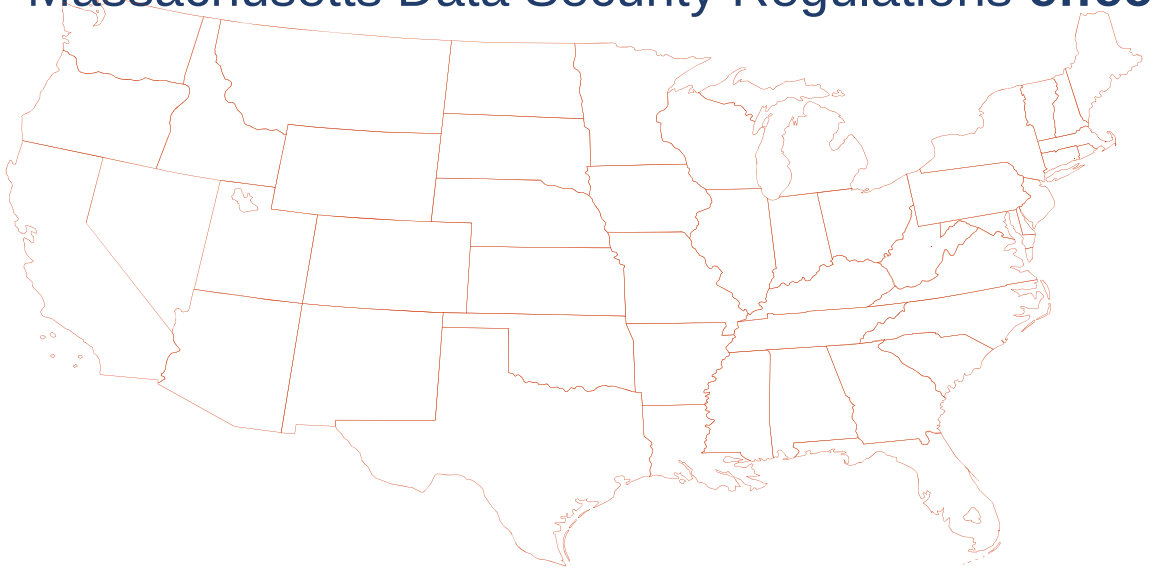
Recent Developments

Red Flag Rules effective Dec. 31, 2010

- Applies to "financial institutions" and "creditors" who have "covered accounts"
  - "creditor" defined broadly and includes businesses/ organizations that regularly defer payment for goods or services or provide goods or services and bill customers later
  - "covered accounts" include:
    - consumer accounts or
    - any account with a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft
- If applicable, required to have a written identity-theft prevention program

State Laws

- 46 states have enacted breach notification laws
  - Most are different!
- 29 states have data disposal laws relating to PII
- Nevada requirements for encryption **effective Jan. 1, 2010**
- Massachusetts Data Security Regulations **effective March 1, 2010**



DuaneMorris

Nevada Amended Encryption Statute

- Encryption requirement
  - must encrypt personal information transmitted electronically outside the “data collector’s” secure system
  - must encrypt personal information stored on any device or medium that is moved “beyond the logical and physical controls” of the data collector or its data storage vendor
- Codifies the Payment Card Industry Data Security Standard (PCI DSS)

Massachusetts Data Security Regulations

- "every person that owns, licenses, stores or maintains personal information" about a Massachusetts resident must have a comprehensive written information security program

- Encryption requirement
  - Transmission of personal information
  - Portable devices (laptop, smart phones, flash drives etc.)

Massachusetts Data Security Program

Develop a security program

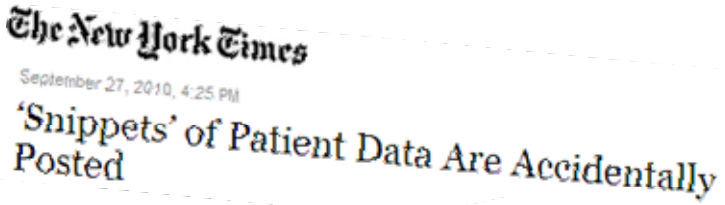
- Assess reasonably foreseeable internal and external risks (including paper or other records)
  - employee training and compliance
- Oversee service providers
  - Careful selection of providers
  - Contractual limitations re: security measures for personal information
- Restrictions upon physical access to records
- Document breaches and investigations

Data Breaches Get The Headlines


COMPUTERWORLD

September 9, 2010 04:42 PM ET

Hotel operator warns of data breach


The New York Times

September 27, 2010, 4:25 PM

'Snippets' of Patient Data Are Accidentally Posted


THE WALL STREET JOURNAL.

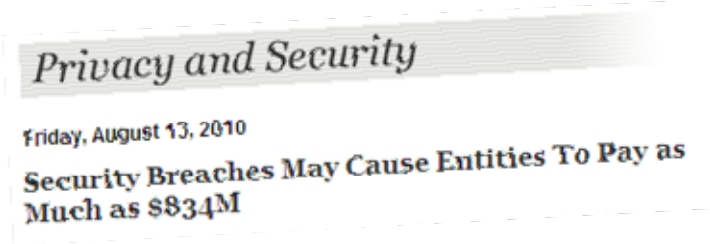
BUSINESS | SEPTEMBER 29, 2010, 12:03 A.M. ET

Data Leak Blindsides Morgan Keegan


HackerJournals

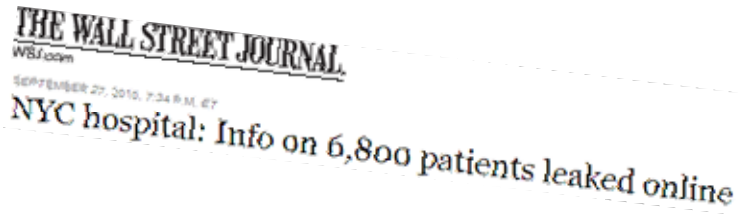
Posted on 22 September 2010

Data security breaches 'on the rise'


Privacy and Security

Friday, August 13, 2010

Security Breaches May Cause Entities To Pay as Much as $834M


THE WALL STREET JOURNAL.

NYC hospital: Info on 6,800 patients leaked online

DuaneMorris

Data Breaches

- The number of breaches continues to rise
- Federal enforcement of breaches escalates
- States take the lead in new laws
- Victims of data breaches continue to face an uphill battle for legal redress
- The cost of a data breach is rising

DuaneMorris

Cost of a Breach

- $204 per compromised customer record in 2009

- Average total per-incident costs in 2009 were $6.75 million

» Data from Ponemon Institute 2010 report

Security Statistics

- Over 70 million security breaches
  - 4% - Lost backup tapes
  - 7% - Unauthorized access to documents
  - 19% - Human Error
  - 25% - Hacking
  - 45% - Stolen/lost computer or portable devices

- Privacy Rights Clearinghouse

High Profile Thefts of Trade Secrets

- Coca-Cola
- Morgan Stanley
- Boeing
- Duracell

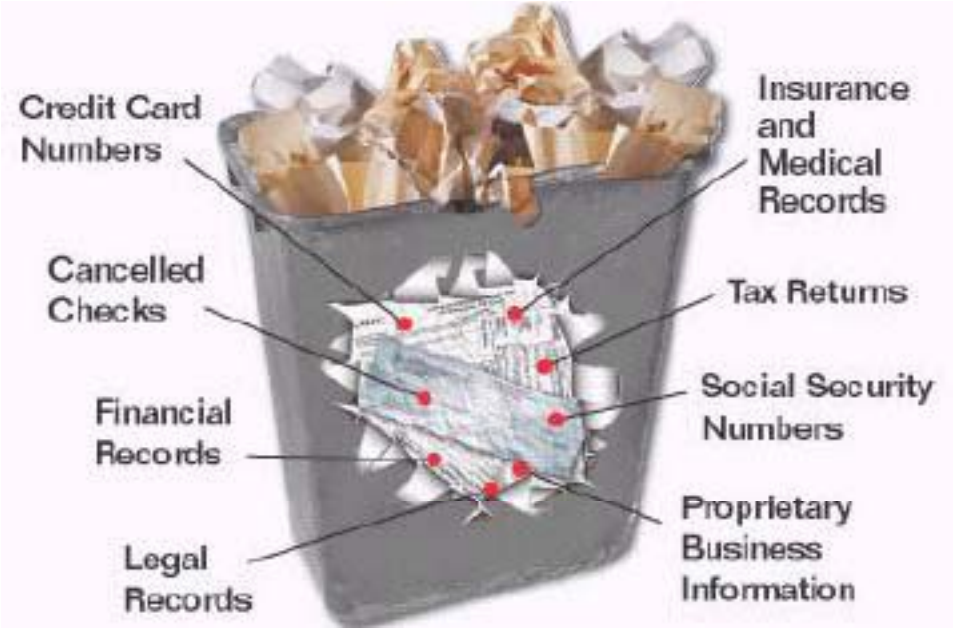
Morgan Stanley

The Threat Within

- Inadvertent disclosures
- Use of unapproved devices
- Carelessness
- Lack of training
- Theft

DuaneMorris

Disposal of Information



Acquisition Related Issues

- Sale of Division, product line or subsidiary
  - Clearly delineate information
  - Protections in acquisition agreement
  - Address possible inadvertent disclosures
    - Employees
    - Systems

Technology Risks to Business

- New storage media
  - Cyberbling
  - MP3
  - Mobile phones
  - Wireless/Bluetooth connectivity
- More tech savvy employees

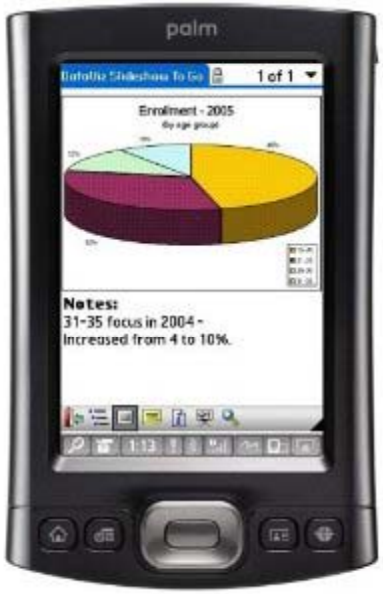
Laptops

Flash/Thumb/USB Keychain Drives

iPhone/ iPod/ MP3

PDAs


Start
12:09
Thursday, September 01, 2005
Tap here to set owner information
No unread messages
No tasks
No upcoming appointments
Tap here to sign in to Pocket MSN!
Device unlocked
Calendar
Contacts

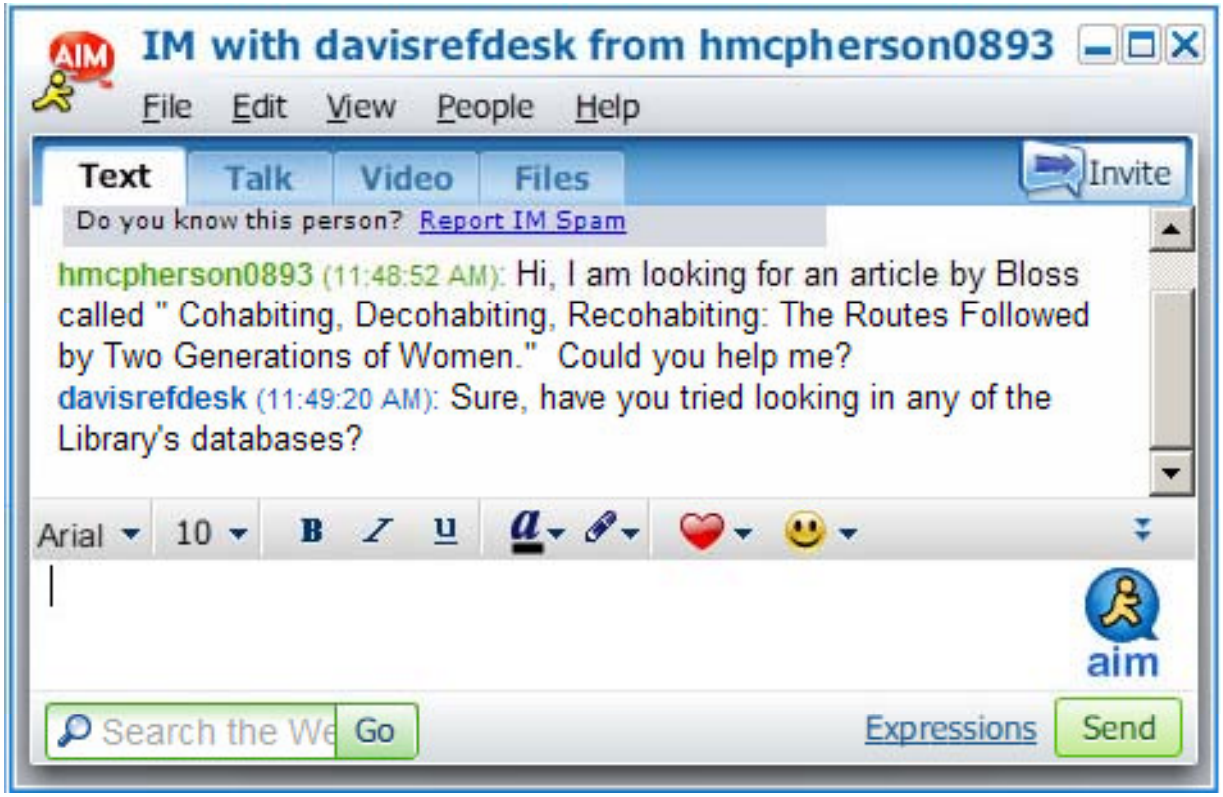

palm
1 of 1
Enrollment - 2005
Notes:
31-35 focus in 2004 -
Increased from 4 to 10%.

Cameras

- Camera phones
- Pen Cameras
- Wristwatch cameras

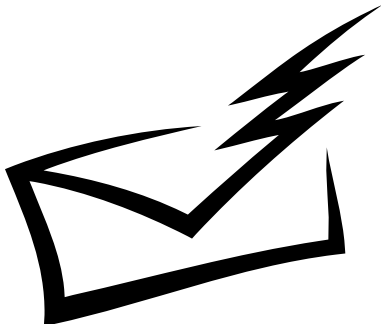
DuaneMorris

Instant Messaging



E-Mail and File Storage

- E-mail sent to personal accounts or put on personal lap tops
- Work files stored on personal devices or web backups
- Inadvertent disclosures by e-mail
  - the Eli Lilly example



Cloud Computing

- Definition:
  - **Narrow**: updated version of utility computing: basically virtual servers available over the Internet.
  - **Broad**: anything outside the firewall is in the cloud, including conventional outsourcing.

Cloud Computing Security Risks

- Most established service providers (Amazon and Google) contract on a take it or leave it basis
- Servers may not be in the US
- Smaller service providers may not survive
- What happens to the data at termination?

P2P software

- P2P Software is installed at least once in 77% of companies

DuaneMorris

FTC Warnings

Fortune 500 Companies and Social Media

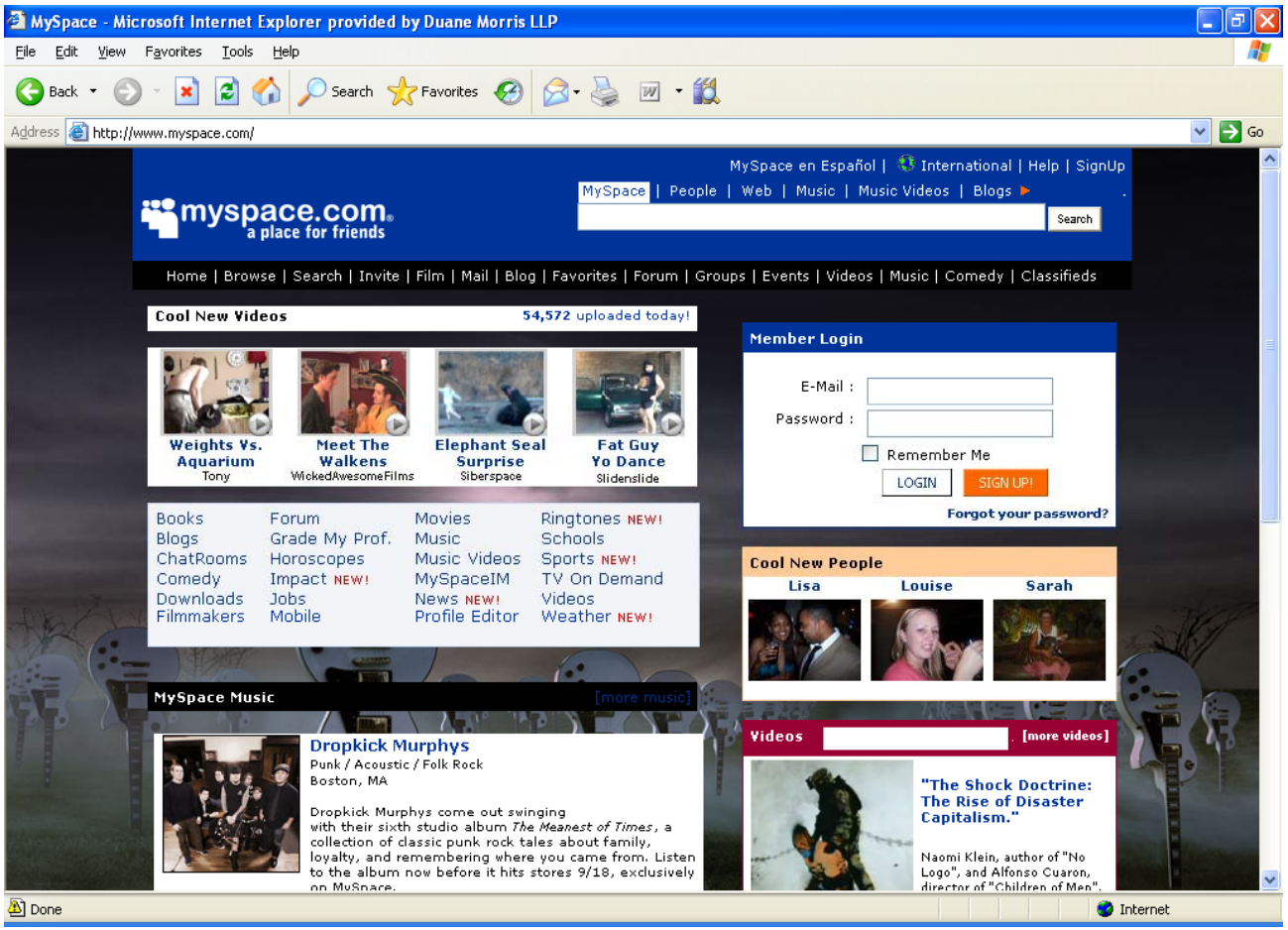
- 22% have blogs (Fortune 500)
  - 31% enhance blogs with video

    (45% of Inc. 500 - fastest growing private companies - have blogs!)

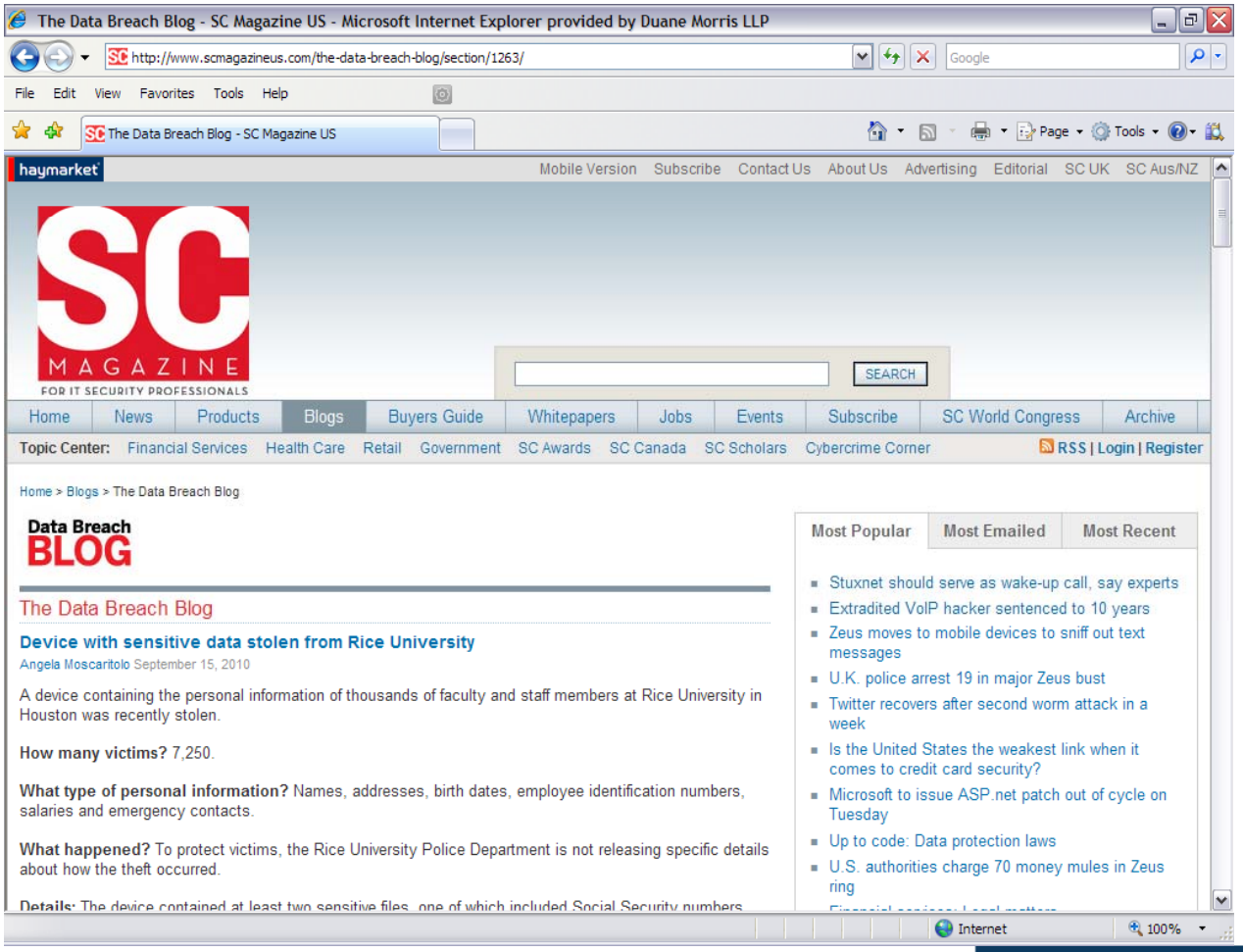
- 35% have a corporate program for tweeting

- 19% host podcasts

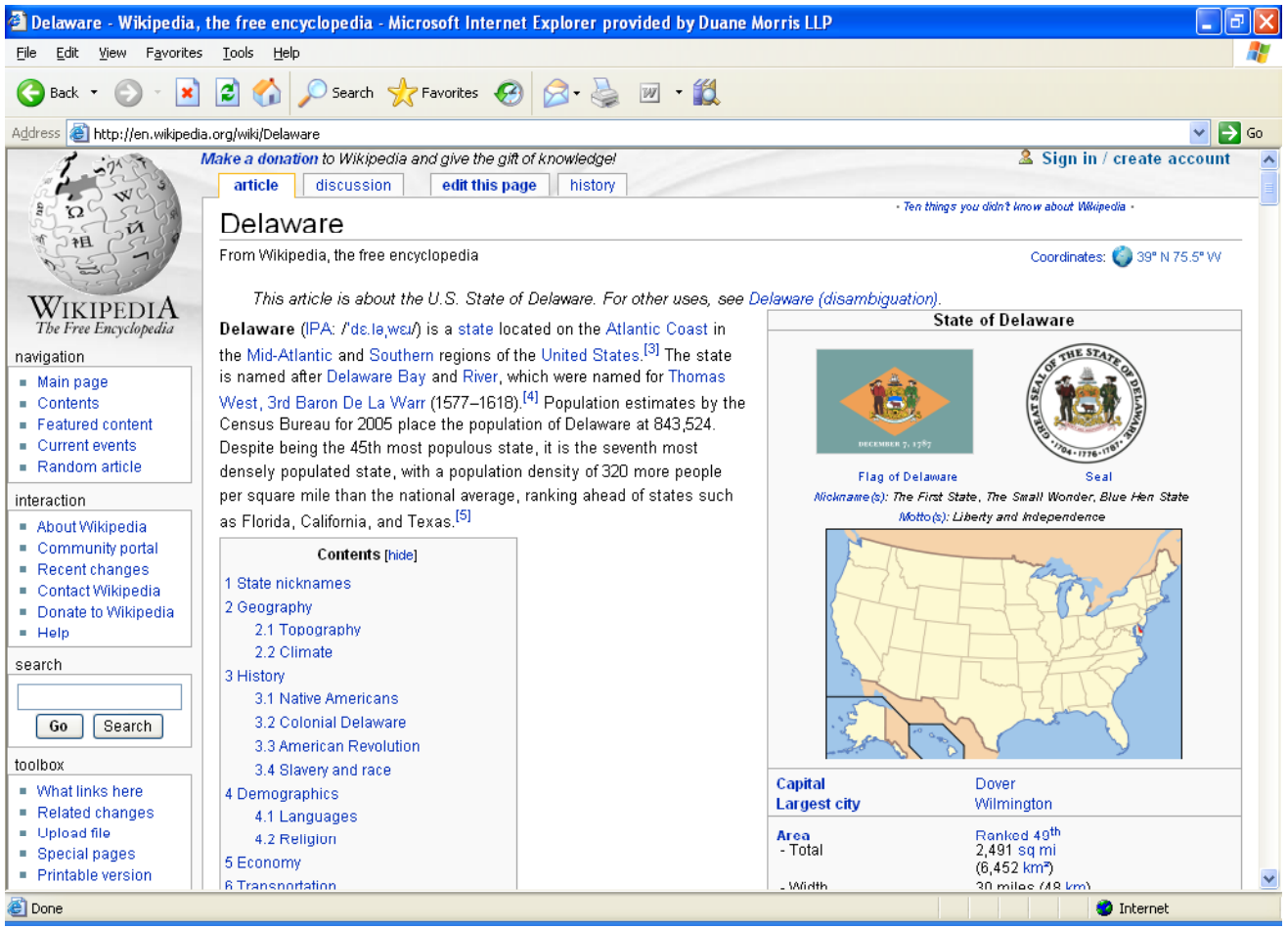
Social Networking Sites – LinkedIn, Facebook, My Space



Blogging


The Data Breach Blog - SC Magazine US - Microsoft Internet Explorer provided by Duane Morris LLP
http://www.scmagazineus.com/the-data-breach-blog/section/1263/
File Edit View Favorites Tools Help
The Data Breach Blog - SC Magazine US
haymarket
Mobile Version Subscribe Contact Us About Us Advertising Editorial SC UK SC Aus/NZ
SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
SEARCH
Home News Products Blogs Buyers Guide Whitepapers Jobs Events Subscribe SC World Congress Archive
Topic Center: Financial Services Health Care Retail Government SC Awards SC Canada SC Scholars Cybercrime Corner
RSS | Login | Register
Home > Blogs > The Data Breach Blog
Data Breach BLOG
The Data Breach Blog
Device with sensitive data stolen from Rice University
Angela Moscaritolo September 15, 2010
A device containing the personal information of thousands of faculty and staff members at Rice University in Houston was recently stolen.
How many victims? 7,250.
What type of personal information? Names, addresses, birth dates, employee identification numbers, salaries and emergency contacts.
What happened? To protect victims, the Rice University Police Department is not releasing specific details about how the theft occurred.
Details: The device contained at least two sensitive files, one of which included Social Security numbers
Most Popular
Most Emailed
Most Recent
Stuxnet should serve as wake-up call, say experts
Extradited VoIP hacker sentenced to 10 years
Zeus moves to mobile devices to sniff out text messages
U.K. police arrest 19 in major Zeus bust
Twitter recovers after second worm attack in a week
Is the United States the weakest link when it comes to credit card security?
Microsoft to issue ASP.net patch out of cycle on Tuesday
Up to code: Data protection laws
U.S. authorities charge 70 money mules in Zeus ring
Internet
100%

Wikipedia


Delaware - Wikipedia, the free encyclopedia - Microsoft Internet Explorer provided by Duane Morris LLP
File Edit View Favorites Tools Help
Back Search Favorites
Address http://en.wikipedia.org/wiki/Delaware
Go
Make a donation to Wikipedia and give the gift of knowledge!
Sign in / create account
article discussion edit this page history
Ten things you didn't know about Wikipedia
WIKIPEDIA
The Free Encyclopedia
navigation
Main page
Contents
Featured content
Current events
Random article
interaction
About Wikipedia
Community portal
Recent changes
Contact Wikipedia
Donate to Wikipedia
Help
search
Go Search
toolbox
What links here
Related changes
Upload file
Special pages
Printable version
Delaware
From Wikipedia, the free encyclopedia
Coordinates: 39° N 75.5° W
This article is about the U.S. State of Delaware. For other uses, see Delaware (disambiguation).
Delaware (IPA: /ˈdɛləˌwɛər/) is a state located on the Atlantic Coast in the Mid-Atlantic and Southern regions of the United States.[3] The state is named after Delaware Bay and River, which were named for Thomas West, 3rd Baron De La Warr (1577–1618).[4] Population estimates by the Census Bureau for 2005 place the population of Delaware at 843,524. Despite being the 45th most populous state, it is the seventh most densely populated state, with a population density of 320 more people per square mile than the national average, ranking ahead of states such as Florida, California, and Texas.[5]
Contents [hide]
1 State nicknames
2 Geography
2.1 Topography
2.2 Climate
3 History
3.1 Native Americans
3.2 Colonial Delaware
3.3 American Revolution
3.4 Slavery and race
4 Demographics
4.1 Languages
4.2 Religion
5 Economy
6 Transportation
State of Delaware
Flag of Delaware
Seal
Nickname(s): The First State, The Small Wonder, Blue Hen State
Motto(s): Liberty and Independence
Capital Dover
Largest city Wilmington
Area
- Total Ranked 49th
2,491 sq mi
(6,452 km²)
Done
Internet

Issues with Social Media

- Leaks of trade secrets and confidential information
- Security breaches
- Financial
- Corporate Reputation
- Regulatory Issues
- Discovery time bombs

Wireless Security

Outsourcing

- "A company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws. . . . Simply because a company chooses to outsource some of its data processing to a domestic or off-shore provider does not allow that company to escape liability for any failure to safeguard information adequately."

Timothy J. Muris, Former Chairman, FTC

Outsourcing and International Risks

- Proving ownership of intangible trade secrets is difficult
- Foreign countries do not always recognize or offer protection for trade secrets in a similar manner
- Foreign countries may not enforce laws

Best Practices in Outsourcing

- Due diligence in outsourcing firms
  - Background checks
  - Review company's history
- Contractual obligations
- Monitoring
- Train partners
- At termination, remove data

The Threat Outside – Competitive Intelligence and Business Espionage

- Business or Economic Espionage
- Industrial or Commercial Spying

Economic Espionage

- The U.S. Attorney General defined economic espionage as:

> "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies."

Economic Espionage and Industrial Spying 2005

Competitive Intelligence

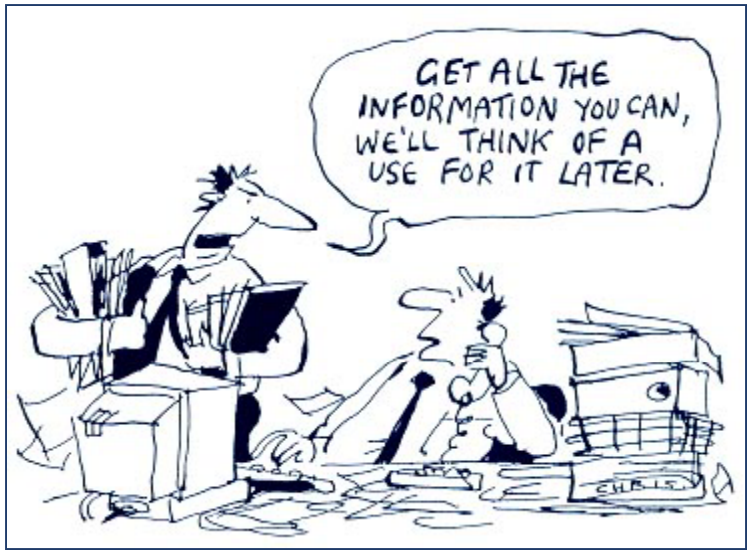
- Competitive Intelligence is defined as:

> "a systematic and ethical program for gathering, analyzing and managing information that can affect a corporation's plans, decisions and operations."

Nasheri, Economic Espionage and Industrial Spying

Examples of Business Espionage

- Maytag “Front Loader”
- Ringling Brothers
- Oracle
- SAP
- HP



Competitive Intelligence

- 90% of large companies have CI staff and many large U.S. businesses spend more than a $1 million annually on CI.

Economic Espionage and Industrial Spying 2005 (citing Business Week 2002)

Legal Collection of Competitive Intelligence

- Public records (on-line databases, industry periodicals, competitors' promotional documents or a review of annual reports, patent filings)
- Trade shows
- Attendance at conferences and seminars
- Analysis of competitor's products
- Customer surveys
- Visual observation of a competitor's site
- Dumpster diving?

Best Practices - Planning

- Identify trade secrets, proprietary information and personally identifiable information
- Conduct a risk assessment
- Draft Policies

DuaneMorris

Best Practices – Policy Development

- Workplace E-Policies and Social Media Policies
- Establish ownership and user guidelines for computer and internet use
- Dispel expectations of privacy
- Obtain employee consent

Best Practices - Policy Development

- Develop a Compliance Plan and Guidelines
  - put employees/contractors on notice
  - include confidentiality provision in contracts and other documents
  - require non-disclosure agreements
  - protect trade secrets and personally identifiable information with passwords, encryption, visitation procedures, locks on file cabinets etc.
  - identify and protect information in *any form*
  - limit access on a need to know basis

Best Practices – Policy Development

- Develop a Data Security Plan
  - Why? Its required!
  - – Comprehensive approach for your most valuable assets
  - – Protection from significant financial loss and damage
  - – Protection of customer information
  - – Contain intrusions, restore systems and provide assistance to customers (if necessary)

Best Practices – Policy Development

- Develop an Incident Response Plan
  - breach containment
  - activation of the core team to handle a breach
  - outline for internal investigation and analysis
  - identification of security breach notification laws
  - notification of relevant authorities and credit bureaus
  - guidelines for internal and external communications
  - media statements

  approach the plan from “when”, not “if”

Best Practices – Policy Development

- Develop a Document Retention Policy
  - Good litigation preparedness tool – e-discovery!
  - Ensures that documents are *properly* destroyed when no longer needed
  - Addresses documents in *all forms*

Best Practices – continued

- Apply all policies and procedures to outside consultants, as well as employees
- Train employees
- Conduct regular audits

Questions?

Protecting Company Confidential or Proprietary Information in the Electronic Age

Sandra A. Jeskie

Partner, Duane Morris LLP

Pamela Lehrer

Vice President and General Counsel
Berwind Group