PRECONFERENCE I: Privacy for Compliance Professionals

Sponsored by the International Association of Privacy Officers

So you want to be a Privacy Professional

Vincent Schiavone, CEO ePrivacy Group
Vice President and Board Member
international association of privacy professionals

iapp

Washington, DC - February 5 - 7, 2003

ePrivacy GROUP™

Overview

- Overview
- Making the Case for a CPO
- The Law and Cost
- Warped Mind of a CPO
- ABC's of a Strong CPO
- “Whole View” Approach
- Getting Started
- Privacy Incident Cost Containment
- Enlightenment
- Training
- CPO Top 10 Tasks
- Conclusions
- Contacts

Ripped from the Headlines

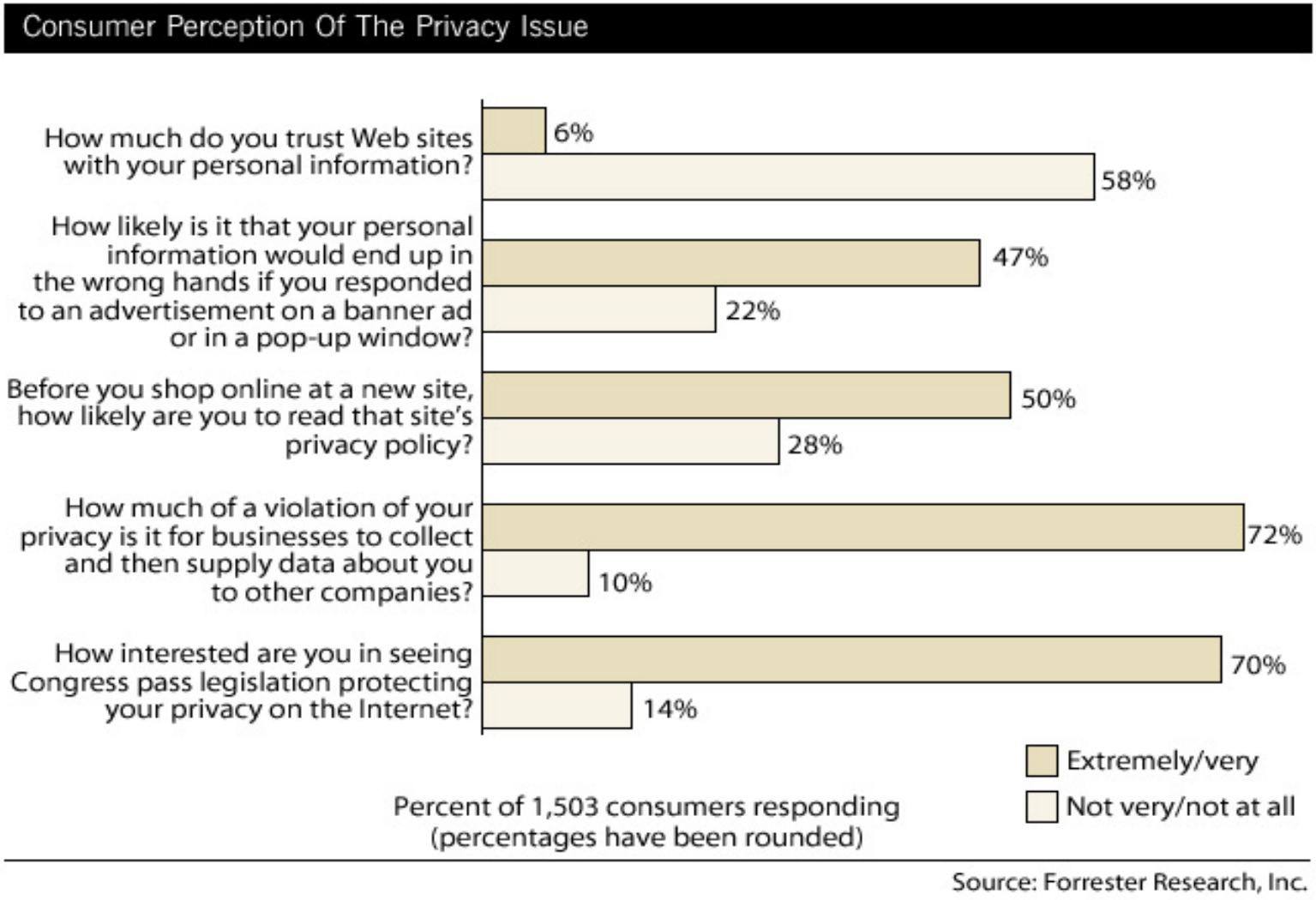
Healthcare will be the next big privacy story

iapp

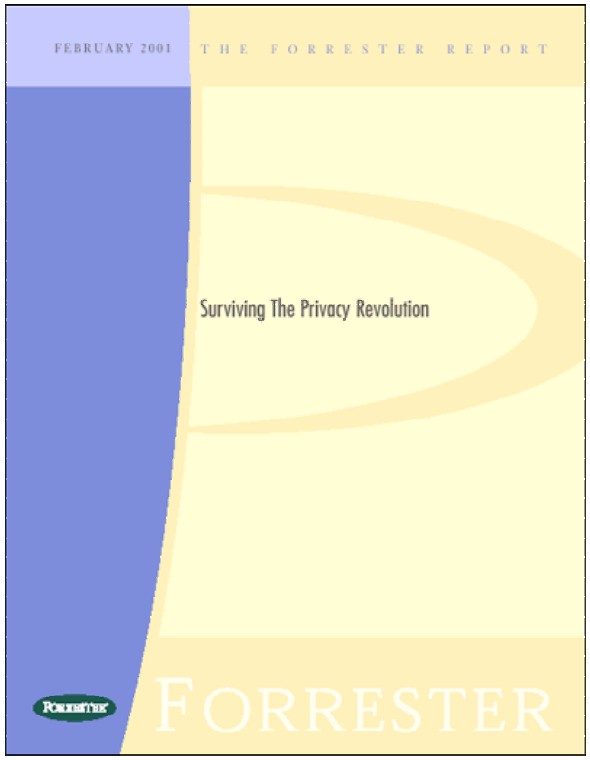
Washington, DC - February 5 - 7, 200

ePrivacy GROUP

Making the Case for a CPO



Making the Case for a CPO – It's the LAW!



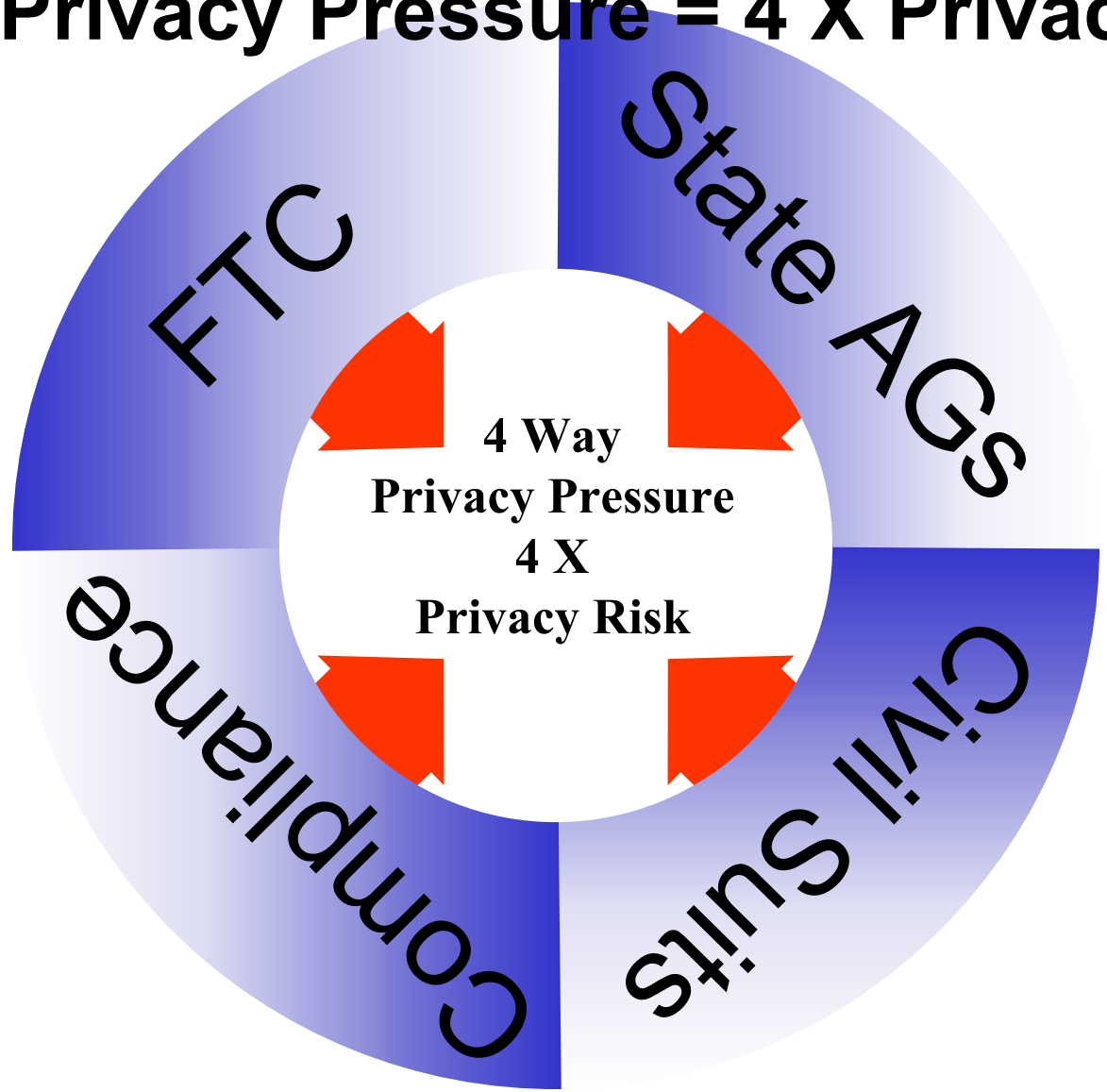
- **"Privacy sensitivity & visibility are intensifying"**
- **"Existing privacy rules already cover most companies"**
  - Of Fortune 100, 73 must comply with at least one set of recent privacy regulations
- **New technologies will keep privacy "wound" from closing**
- **Regulatory labyrinth will worsen**
- **Conclusion: "Whole View" approach to Privacy is required**

Three "Types" of Laws

- Established Laws
  - Fed, State, International
  - FIPP
  - EUDPD
- Emerging Laws
  - HIPAA
  - "New" Enforcement Actions
  - "New" Civil Suits
  - Your are responsible for your vendors
- Law of the Press
  - Company is ALWAYS wrong
  - Consumer is NEVER wrong
  - Your are responsible for your vendors

Press is driven by brand – your brand

4 Way Privacy Pressure = 4 X Privacy Risk



Risk: Cost of Privacy Incidents - Escalating

2000

Small.com, Inc. Action	Time (hours)	Cost
• CEO/president time	86	$7,100
• Management time	95	$5,544
• PR meetings and calls	40	$1,067
• Management press calls	26	$1,778
• Management review of privacy practices	15	$833
• Customer service calls and emails	88	$1,944
• Employee communications and training	1	$1,333
• External consultants		$22,500
• Travel		$2,000
Grand total		**$44,099**

BigCompany, Inc. Action	Time (hours)	Cost
• CEO/president time	48	$8,100
• Management time	620	$38,889
• PR meetings and calls	800	$21,333
• Management press calls	76	$5, 456
• Management review of privacy practices	250	$13,889
• Customer service calls and emails	18,750	$416,667
• Employee communications and training	18,770	$335,889
• External consultants		$181,250
• Travel		$16,500
Grand total		**$1,037,973**

2002 add FTC settlement
20 Yrs monitoring
State Attorneys General
Civil Suits

Sub	**~ $ 2,000,000,00**
`Total	**~ $ 3,000,000.00**

WHY are Costs Rising?

DoubleClick

Eli Lilly

Microsoft

Ziff-Davis

USBancorp

Eckerd

When Companies Make Privacy Mistakes

- **Eli Lilly Prozac Email Incident**
  - FTC settlement, lasts 20 years
  - State fines
- **Microsoft Passport**
  - FTC settlement
  - Fines if broken ($11K per incident)
- **Doubleclick**
  - Class action, FTC, $400K states
- **Ziff Davis**
  - Exposed credit cards on Web,
  - Identity theft resulted, $125K to states
- **Eckerd Drug**
  - Drug signature sheets as permission to market—settled with Florida AG for $1 million (endows a university chair in Ethics)

Consider the Fallout:
Stock price takes a hit
Press "goes negative"
Brand name tarnished
Resources diverted
Opportunity costs mount
e.g. Marketing, PR, Staff, Managers, Lawyers

Training Specified in Privacy Settlements

- Microsoft: this risk assessment should include consideration of risks in each area of relevant operation, including:
  (1) employee training and management…
- Ziff Davis: address these risks by means that include:
  (i) management and training of personnel…
- DoubleClick: will undertake reasonable efforts to educate its clients in technical and business practices that promote Users' privacy…. will employ reasonable technical and employee education procedures and mechanisms to safeguard the security and integrity of User Data…
- Eli Lilly: including any such risks posed by lack of training, and addressing these risks in each relevant area of its operations, whether performed by employees or agents…

So you STILL want to be a CPO?

What it takes to do it right

The Warped Mind of a CPO

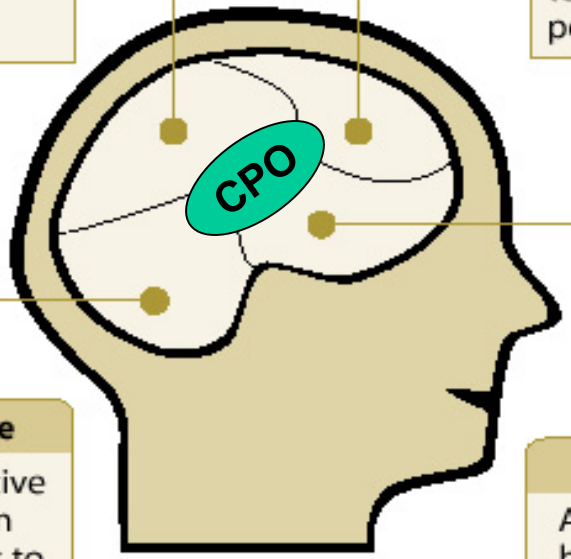
The Mindset And Various Skills Of A Chief Privacy Officer

Attorney

Compliance -- must know how to navigate through the patchwork of both US and international privacy regulations

IT specialist

Thorough knowledge of the capabilities and limits of technologies that manage personal data



Generalist Communicator

CPO - Privacy Advocate for

- **Corporation**
- **Customers**
- **Employees**

Public relations executive

High internal profile; proactive reassurance of consumers in sensitive markets; readiness to counter privacy blowups

Marketing manager

Ability to vet new products and business deals or alliances for privacy problems that other executives might disregard

Source: Forrester Research, Inc.

The ABCs of a Strong CPO

- **Accountability & Authority**
  - CPO responsible for all aspects of corporate privacy
  - CPO must have authority if accountable
- **Breadth of Influence & Budget**
  - Able to get a "big picture," strategic view of today's operations and tomorrow's planning
  - Positioned in company to review all operational areas
  - Institutionalized as a part of the decision process for any activities involving gathering, use of PII
  - Own budget
- **Clout**
  - Positioned on org. chart as peer to key managers
  - Strong backing of CEO and Board

What the "Whole View" Approach Means

- First, Company must recognize that privacy is a core issue in all dealings with customers – It's about TRUST
- Second, development of a coordinated privacy strategy requires top-to-bottom assessment of online and offline data gathering and usage
- Whole View requires Four Pieces:
  1. An empowered CPO
  2. Discover and document the flow of PII
  3. Develop privacy policies and procedures
  4. Institutionalize privacy protection measures

1. An empowered CPO

Tasks:

- Build a privacy team
  - Recruit a *de facto* team from key departments

  Example: 3000 person consumer facing company, 40 privacy
- Strengthen your influence base
  - "Privacy Committee" CPO often not a "C" or an "O"
  - Strength = support from above
- Compliance is key
  - Understand the processes, technologies
  - If you don't, hire someone who does
- Avoid becoming a bottleneck
  - Learn the alternatives
  - …but hold your ground when you're right.

2. Discover and document the flow of PII

Tasks:

- Prevention – Target, Treat, Train –
  - Practical Privacy – fix the obvious
  - PICC – Privacy Incident Cost Containment
- Key areas: IT, HR, Marketing, Vendors
- Survey the entire corporation
  - If you can't do it in-house, decide who's going to help
- Document data sources, uses, access policies
- Identify current and potential problem areas

3. Develop privacy policies and procedures

Tasks:

- Assemble current policies and assess inconsistencies
- Benchmark against
  - Applicable laws, regs
  - Industry standard practices
- Draft a unified privacy policy, key SOPs
- Assess obstacles to implementation
  - Prioritize implementation to address worst exposures first
- Craft a public privacy policy document
  - Don't let the lawyers do the first draft
  - If you have a lousy policy, say it proudly

4. Institutionalize privacy protection measures

Tasks:

- Instill a culture of privacy in the corporation
  - Culture starts from the top down
  - Compliance starts from the bottom up:
  - Training is the key
- Set up internal monitoring procedures
  - Implement procedures for regular review of PII systems
  - Implement regular internal and external audits
  - Don't forget 3rd party service providers, partners
- Prepare for blowups - Contingency planning
  - Recognize, React & Respond
    - Develop an investigatory process
    - Develop a PR plan
    - Involving privacy advocates early builds credibility

Getting started?

Be smart, be fast, be practical

Manage today's risk – Today!

Privacy incidents & investigations

Bad questions to have to answer

- **"What did you know?"**
- **"When did you know it?"**
- **"Why didn't you know sooner"**

Really bad questions to have to answer

- **"Why didn't you act after you new?"**
- **"How long didn't you act after you new?"**

- **Tip: Always be truthful – there is always a trail**

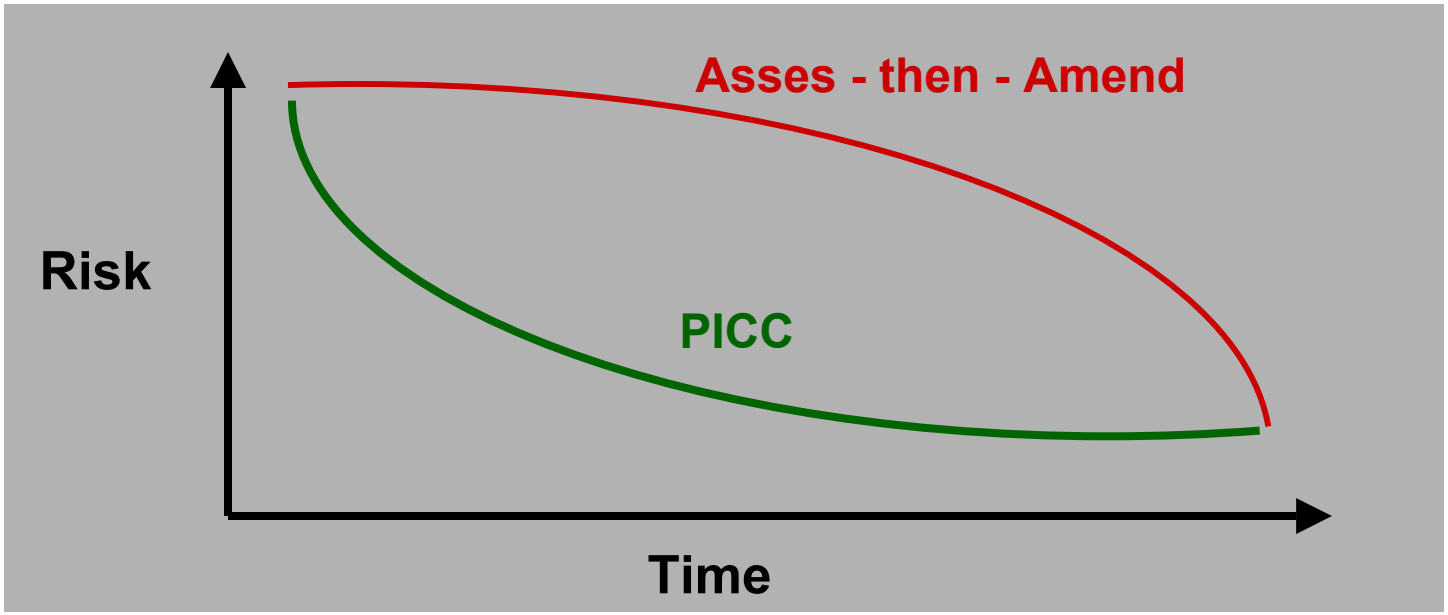
Practical Privacy: Triage - fix the obvious!

3-step Privacy Incident PREVENTION Program

1. **Target**
   - Find current privacy exposures and prioritize
   - (Talk to department heads, map data flows, ask questions, especially of marketing)
2. **Treat**
   - Make necessary changes and then institute policies and procedures to prevent recurrence
3. **Train**
   - Train yourself, IAPP, train your team, train your boss
   - Make sure everyone understands the importance of privacy, especially anyone who touches PII
   - (This goes a lot further than customer service, e.g. contracts, programming, product development)

Privacy Incident Cost Containment Model

- **"Asses-then-Amend" prolongs risk of privacy incidents**
  - Can actually increase risk
- **PICC reduces privacy risks right away**
  - Resources immediately applied against risk



CPO Enlightenment

1. There is no magic technology solution
   - Part of the solution
2. There is no magic legal notice
   - Backlash against legalese
3. You can't do it alone
   - Lots of Privacy touch points
     - Eli Lilly Florida
   - New exposures created
4. You can't do it without budget
5. Vendors are your privacy responsibility

Train your team - Train ALL potential touch points

Train your vendors

HIPAA Training – Set Expectations

TRUSTe PRIVACY TRAINING

Health Privacy Module A:
Health Privacy Awareness

1 of 10
26 Mar 2002

Health Privacy Awareness

- The purpose of this class is to help you deal more effectively and appropriately with issues of health privacy that arise in your work
- Answer questions
  - What are health privacy issues?
  - When do they arise?
  - What is HIPAA?
  - What does it mean to your company and your job?
- Increase your health privacy awareness
  - Spot problems before they occur
  - Solve problems by doing the right thing
- Understand how good health privacy practice makes good company practice

Increasing health privacy awareness and understanding makes for better business

ePrivacy GROUP | BANK INC.

Home Save Audio Back Next Help

HIPAA Training – Don't Skip Why

TRUST·e PRIVACY TRAINING

Health Privacy Module A:
Health Privacy Awareness

7 of 10
26 Mar 2002

What the Heck's a HIPAA?

- The Health Insurance Portability and Accountability Act of 1996
- An attempt to make health insurance easier and cheaper by using electronic data interchange technology (EDI)
- EDI saves money if you have standard codes for processes such as billing, and HIPAA standardizes health care codes
- Assumes more use of computers in health care, and so a need to protect the privacy of patient data, hence:
  - HIPAA Privacy Rule
  - Effective April 14, 2003
- Requires policies and procedures for handling PHI, protected health information
- There are stiff fines for violations

HIPAA makes protection of health information a part of Federal law.

ePrivacy GROUP | BANK INC.

Home Save Audio Back Next Help

Why? – Increased Sensitivity

TRUSTe PRIVACY TRAINING

Health Privacy Module A:
Health Privacy Awareness

4 of 10
26 Mar 2002

Why Is Health Privacy Such An Issue Today?

- The idea that people who handle health information should respect the privacy of individuals is not new
- But people today more concerned about possible threats to their privacy as a result of developments in computers and communication
- Computer networks make gathering and sharing information easier than ever and some of that information is IIHI
- Health privacy is impacted by the extensive use of computers in health insurance, payment, research, and marketing

People have always been concerned about privacy,
but today's level of concern about health privacy is unprecedented

ePrivacy GROUP BANK INC.

Home Save Audio Back Next Help

Compliance is a Business Need

TRUSTe PRIVACY TRAINING

Health Privacy Module A:
Health Privacy Awareness

3 of 10
26 Mar 2002

Privacy Acronyms

Privacy, like other aspects of business, has its own terminology and acronyms. This is particularly true of health privacy. Here are four that you are bound to encounter:

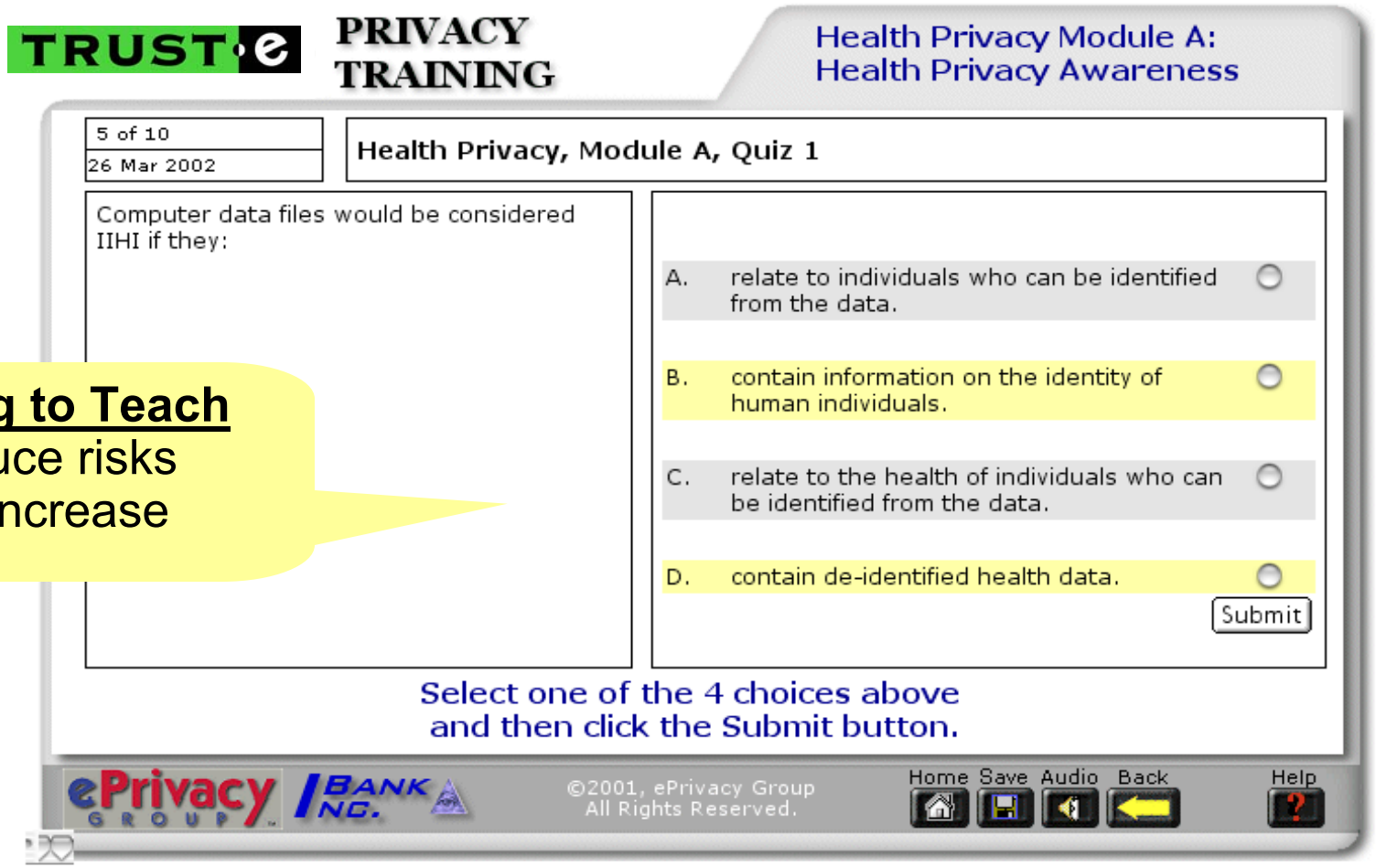
- PII = Personally Identifiable Information
  - Information that relates to an individual who can be identified, directly or indirectly, from the data, particularly by reference to an identification number or aspects of his or her physical, mental, economic, cultural, or social identity
- IIHI = Individually Identifiable Health Information
  - Like PII, but referring specifically to a person's health information
- PHI = Protected Health Information
  - This is a sub-set of IIHI which requires special attention under HIPAA
- HIPAA = Health Insurance Portability and Accountability Act
  - Federal legislation which, among many other things, requires protection of an individual's health information

Privacy acronyms can be a useful shorthand,
but don't assume everyone knows what they mean

ePrivacy GROUP | BANK INC.

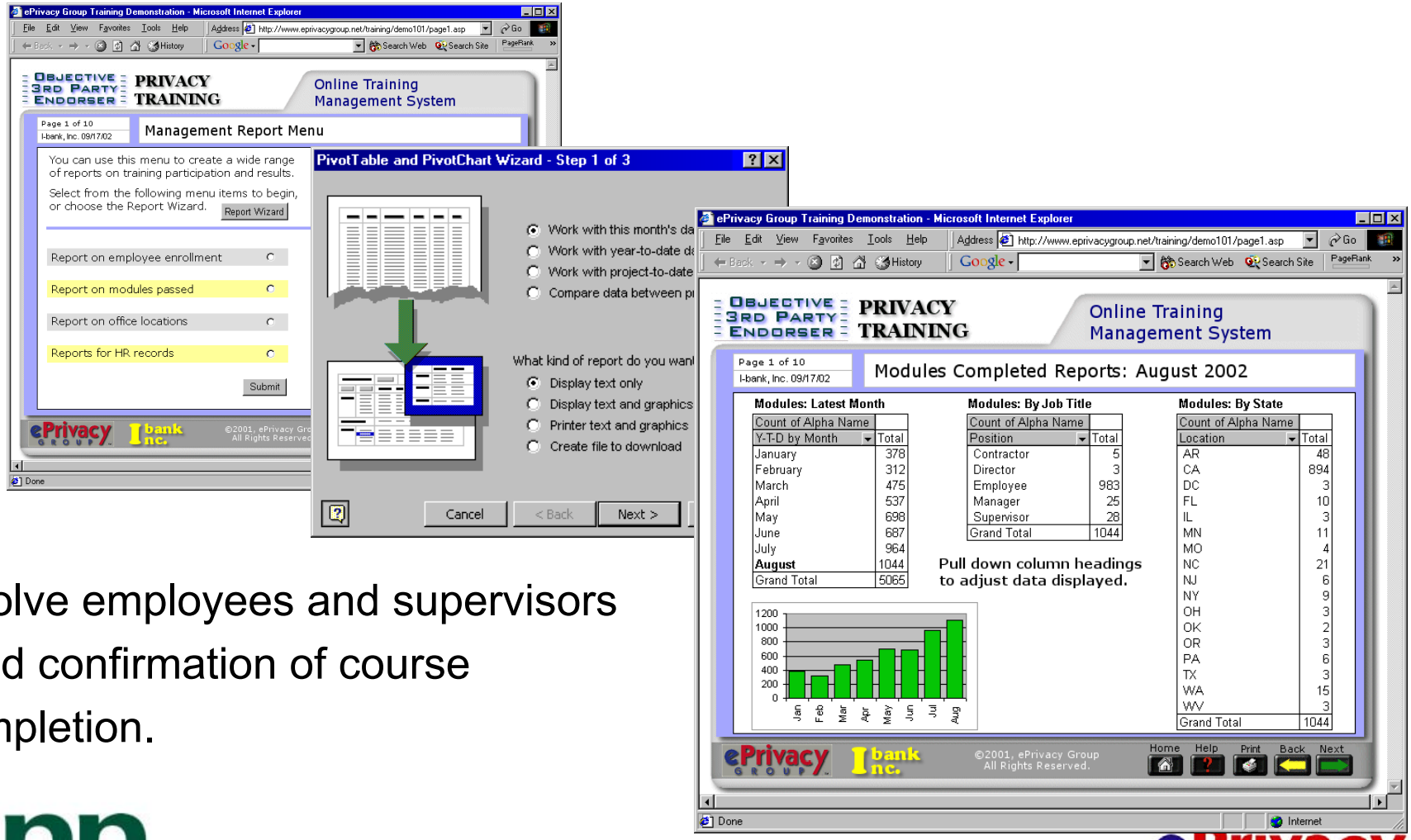
Home Save Audio Back Next Help

Quizzes for Learning and Measuring



Testing to Teach
Reduce risks
not increase

Document Compliance



Involve employees and supervisors send confirmation of course completion.

Acknowledge Employees with Certificates

CPO's Top Ten Challenges

1. Data = corporate "family jewels," but value = use
2. Contractual protections helpful, but not enough
   - breach, leakage
3. Security threats: hackers & the marketing dept.
4. New products/services requiring review of data policies
5. New partnerships/alliances requiring coordination of policies
6. Data "bumps" (combining databases, augmenting data)
7. M&A issues (merging differing policies), Bankruptcy
8. Monitoring for compliance in fast-moving organizations
9. Consumer fears as high as ever, media enjoys feeding fear
10. Legislators/regulators eager to turn that fear to their advantage

Conclusions

- **Embracing Privacy is a corporate necessity**
- **A "Whole View" approach is required**
  - Addressing Privacy begins with a strong CPO or CPP
  - Practical Privacy – fix the obvious
    - Target, Treat, & Train
  - Assessing the data flow is key to understanding exposures and liabilities
  - Establish policies and procedures
  - Institutionalize privacy protection

Conclusions

- **Incidents will happen**
  - Plan for blow-ups
    - Recognize, React & Respond
    - Scenario planning effective way to get attention & budget
- **Training is the key for Prevention & Response**
    - It works
    - Single most effective means to reduce risks

Contacts

IAPP – international association of privacy officers

www.privacyassociation.org 800-800-266-6501 Fax: 215-545-8107
information@privacyassociation.org

ePrivacy Group

- **Ray Everett-Church, Esq., Chief Privacy Officer**
  ray@ePrivacyGroup.com
  +1 703.627.2361
- **Michael Miora, CISSP, Sr. VP & Managing Director**
  mmiora@ePrivacyGroup.com
  +1 310.306.0111
- **Vincent J. Schiavone, President & CEO**
  vs@ePrivacyGroup.com
  +1 610.407.7083