

Protecting your Business and Maintaining Your Customer's Trust

March 11, 2008

Eric Nelson, CIPP

Principal – Privacy and Information Security



enelson@SecurePrivacySolutions.com
www.SecurePrivacySolutions.com
949-721-5897

©2008, Secure Privacy Solutions, All rights reserved.

Almost every firm faces significant risks
relating to data breaches and ID theft.



What can I do to protect my business and maintain the trust of our clients?



The question isn't "if" it will happen to your company, but "when".



You want to mitigate your risks and protect your clients.



Copyright 2008, Secure Privacy Solutions.
All rights reserved.

Risks



Requirements



Solutions



Risks

Data breaches and ID theft are at an all-time high.



Theft of personal data more than triples this year.

Over **162 million** records reported lost or stolen in 2007

49.7 million went missing in 2006.



Computers don't lose or steal data, people do.



People – Illegal Immigration



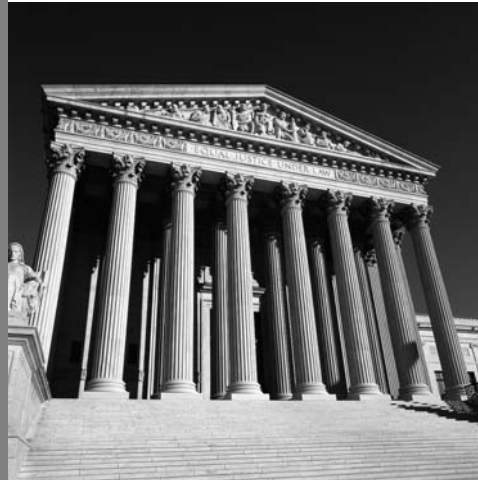
People - Financial gain



People - Carelessness



Current Laws



Low risk to criminals – perceived as non-violent crime.



Current laws impede investigations



Minimal sentencing guidelines



Investigation Challenges



Jurisdictional issues



Business and Individual Cooperation



Resource Restraints



Requirements

You are required to properly handle your customer and employee information.

Betsy Broder: The FTC will act against companies that don't protect customers' data.



"Stolen Lives" ABA Journal, March 2006



You have to be aware of governance and compliance requirements.



FACTA

Fair and Accurate Credit Transactions Act of 2003



FTC settlement under the Disposal Rule: \$50,000

"on at least two occasions, additional intact American United documents containing consumers' personal information were found in and around the same dumpster adjacent to American United's office."



Gramm-Leach-Bliley Act



Severe civil and criminal penalties for noncompliance, including:

- Civil penalties up to \$100,000 for each violation
- Key officers may be fined up to \$10,000 per violation.



International Privacy Laws



You have to be aware of state and federal requirements and enforcement.



Federal Trade Commission



Unfair Trade Practices

Deceptive Trade Practices



State Regulations and Agencies



Pending Legislation



You have to be aware of the implications of non-compliance.



Financial Risks



Loss of Customer Trust



Loss of Company Value



Solutions

Protecting your business and your customer's trust.



Assess your information flow and prioritize risks.

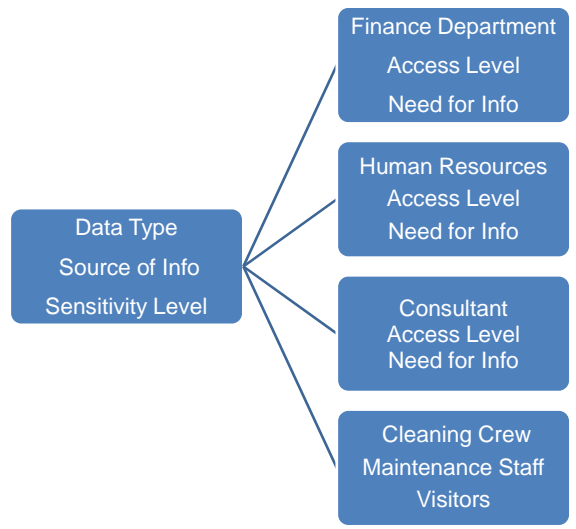


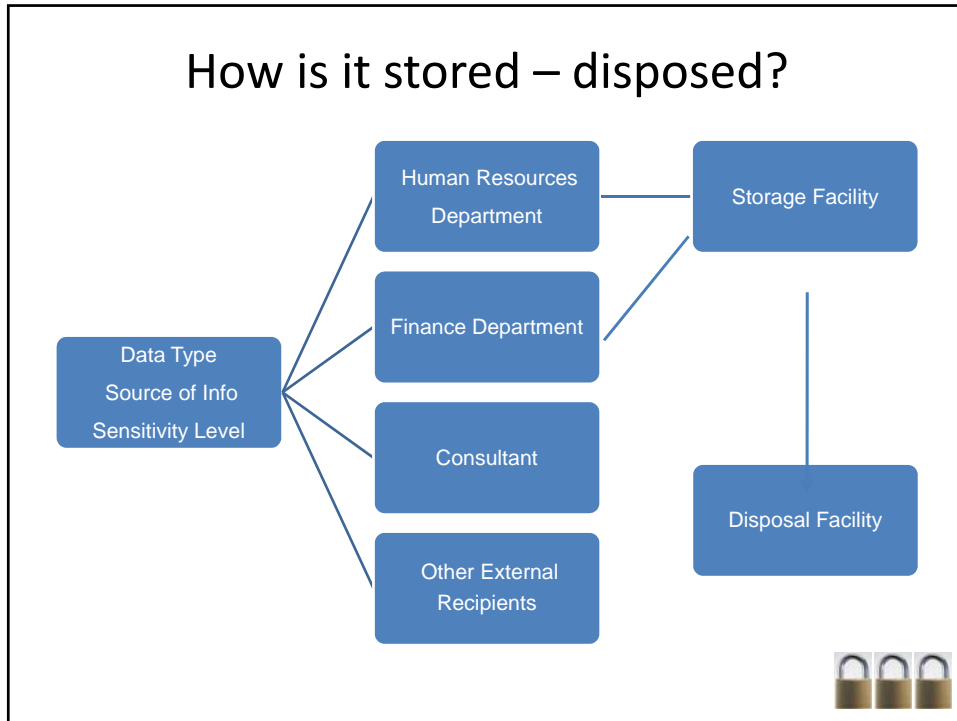
What info is being collected?

Data Type
Source of Info
Sensitivity Level
Why is it being collected?
Is it necessary to collect?
How is being used?



Who has access to info and why?





Policies
Accountability
Awareness

The image shows a computer monitor with a large, heavy-duty metal chain wrapped around its top and sides. A large padlock is attached to the chain, symbolizing security and protection of information. In the bottom right corner of the image area, there are three small padlock icons.

Privacy and Safeguard Policies



Accountability



Role-based Training & Awareness



Plan for
Worst Case



The Storm is Here



Breach Notice Act

CA SB 1386

Personal info triggering notice

Name *plus* one of the following:

- SSN
- Drivers license number
- CA identification number
- Financial account numbers

Applies to “unencrypted, computerized” data

Best practice is to notify in cases of breaches of notice-triggering information, no matter what format.

- Paper and digital data

Recently includes medical information

Whom to Notify

Notice must be given to any data subjects who are CA residents

How to Notify

Writing, electronically or by substitute notice

Substitute notice may be used if:

- Cost of individual notice is over \$250k
- More than 500k people affected
- You do not have contact information



Incident Response - Preparation



Identify your Incident Response Team

- Roles and responsibilities

Develop response policies and plan

- Priorities and approach
- Departmental procedures
- Customer response
- Containment and control

Communicate and evaluate

- Training
- Audit of effectiveness

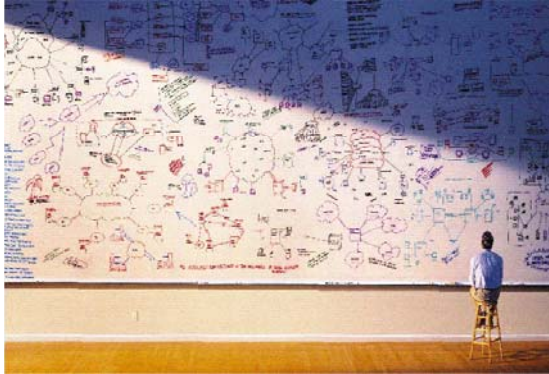


Presentation Summary

- Understand risks that face your business
- Understand regulations that affect your business
- Develop policies, train employees and prepare for the worst to protect your business and maintain your customer's trust.



Questions



Eric Nelson
Certified Information Privacy Professional
enelson@SecurePrivacySolutions.com
www.SecurePrivacySolutions.com
949-721-5897

Copyright 2008, Secure Privacy Solutions.
All rights reserved.

Disclosure

This information does not represent legal counsel or legal interpretation. It is provided as a guide to help companies understand the risks associated with privacy issues.

Secure Privacy Solutions or any of its members do not make any warranties, guarantees or representations about the fitness for any purpose of the privacy policies and related materials found in this overview.

Copyright 2008, Secure Privacy Solutions.
All rights reserved.