Information Security & Privacy:
An Issue at the Heart of Business and Technology Convergence

Sharon O’Bryan, President & CEO
O’Bryan Advisory Services, Inc.
skobryan@obbi.com

October 3, 2003
University of Minnesota
Carlson School of Management
MIS Research Center
Agenda

8:30 – 9:30
Open Introductions
Goals
Privacy Foundation

9:30 – 9:40
Break

9:40 – 11:00
Security Foundation
G-L-B-A Key Points
HIPAA Key Points
Summary
Introductions
Seminar Participants

- Name
- Company
- Responsibility for Privacy/Security
- Exposure to technology aspects of Privacy/Security
- Goal
Goals
Goals

- Explore privacy issues from multiple perspectives
- Establish a mental framework to create solutions to reduce privacy exposures
- Understand technology-induced exposures to privacy
- Understand requirements as prescribed by the Gramm-Leach-Bliley Act 501(b)
- Understand requirements as prescribed by the Health Insurance Portability and Accountability Act of 1996
- Realize applicability to participants through hypothetical case studies
- Explore privacy matters from multiple perspectives:
  - Citizens
  - Business Leaders
  - Investors
Privacy Foundation
Privacy in Context

- Industry
- Company/Business
- Within the context of G-L-B-A
  - Sec. 501
    - “...customer’s non-public personal information”
- Within the context of HIPAA
  - Standards for Privacy of Individually Identifiable Health Information
    - Protecting the privacy of health information given the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996
- Collection, Use and Disclosure of Personal Information
High Level Considerations

- **Operationally**
  - Transaction
    - Documents
    - Printouts
    - Verbal Communication
  - Customers
  - Business Partners
  - Vendors
  - Consultants
  - Auditors

- **Technically**
  - Transaction
    - Creation
    - Maintenance
  - Network traversing
  - Application
  - Database
    - ALL Platforms
  - Storage
    - Temporary Storage
    - Backups
    - Diskettes
    - CDs
    - PCs

Transaction Flow Diagram is *essential* to ensuring consistent, end-to-end, protection of information
Group Participation

- Applying for a mortgage
Group Participation

- Taking a STD Leave from work
Group Participation

- Changing your health insurance to add a new family member

- 

- 

- 

- 

- 

- 

- 

- 

- 

-
Group Participation

- Obtaining a life insurance policy (external to your employer)
Group Participation

- Charging a purchase at a store
Group Discussion Summary

- What are your concerns as a consumer
- How do they apply to your company?
Information Assets & Rights

- **Consumer**
  - What do you consider your personal and confidential information?
  - Who has it?
  - What are your expectations around “the custodian’s” control of it?
  - How do you verify compliance?
  - What information do you expect to be shared to enable service offerings to you?

- **Business**
  - How has your business identified customer confidential/critical information?
  - How has your business identified critical corporate information?
  - How does your business identify this information?
  - How are employees expected to handle this information?
  - How does the management verify employees are aware and capable of delivering upon expectations?
Update Risk Assessment

- The **value** of the information drives the risk.
- Business operations executives are **guardians**, or **owners**, over information & define the **classification** to be assigned to the information within the context of **risk**.
- The **classification** drives the access, handling, marking, retention, audit trail, and investment associated with the information.
Risk Assessment Process

- General Information
  - Project View
  - Business Process View
- Information Classification
- Business Continuity Classification
- Resource Classification
Information Classification

- "Unrestricted"
  - Information generally known; no marking or special handling required.

- "Restricted"
  - Information has proprietary value; must be marked and available only to those authorized to execute related transactions.

- "Confidential"
  - Information with significant proprietary value with relatively minimal distribution need; access logged.

- Now think about this from a consumer’s view!
## General Information

*From a PROJECT perspective, the Project Manager would be responsible for the completion of this section.*

### 1. GENERAL/PROJECT INFORMATION

<table>
<thead>
<tr>
<th>Project Name:</th>
<th>Project #:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Case #:</td>
<td>CORP#:</td>
</tr>
<tr>
<td>Approved Date:</td>
<td>Start Date:</td>
</tr>
<tr>
<td>Executive Sponsor:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Business Owner:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Project Manager:</td>
<td>Phone:</td>
</tr>
<tr>
<td>IT Application Owner:</td>
<td>Phone:</td>
</tr>
<tr>
<td>CRM Representative:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Project Description:</td>
<td></td>
</tr>
</tbody>
</table>
General Information

From a Business Process perspective, the Business Owner would be responsible for the completion of this section.

<table>
<thead>
<tr>
<th>1. GENERAL/ PROJECT INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Transaction Description:</td>
</tr>
<tr>
<td>Division/Department Name:</td>
</tr>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>Division Executive Print/Signoff:</td>
</tr>
<tr>
<td>Business Owner Print/Signoff:</td>
</tr>
<tr>
<td>Key Data Field 1:</td>
</tr>
<tr>
<td>Data Field 2:</td>
</tr>
<tr>
<td>Data Field 3:</td>
</tr>
</tbody>
</table>

Customer Service Level Description:

Regulatory Implications:
## 2. INFORMATION ASSET CLASSIFICATION

Instructions: Using the definitions provided, check only **ONE box** on each row to indicate the **highest** level of risk appropriate to the information assets affected by this project. Provide justification for your selection.

*NOTE*: An incident is defined as a harmful event such as unauthorized modification of data, inappropriate disclosure of information, or unavailability of information or information systems.

<table>
<thead>
<tr>
<th>ATTRIBUTE / CLASSIFICATION</th>
<th>UNRESTRICTED An incident affecting the information asset may cause little or no damage to the company.</th>
<th>RESTRICTED An incident affecting the information asset may cause significant damage to the company.</th>
<th>CONFIDENTIAL An incident affecting the information asset will probably cause substantial damage to the company.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RELIABILITY</strong></td>
<td>The business requirement to have accurate, complete, and timely information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification for Reliability Classification:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AVAILABILITY</strong></td>
<td>The business requirement to access the information at specific times.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification for Availability Classification:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CONFIDENTIALITY</strong></td>
<td>The business requirement to protect information against unauthorized disclosure, whether accidental or deliberate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification for Confidentiality Classification:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. BUSINESS CONTINUITY CLASSIFICATION

Instructions: **Check only ONE box on each row** to indicate the impact on the customer, operations, and regulatory or legal requirements if the application or function were interrupted once this project is implemented. **THIS MATRIX DOES NOT REPLACE THE BIA; it is intended to bring business continuity issues to light during the early stages of the project. For more information, contact the Business Continuity Planning and Technology Recovery group of Technology Risk Management.**

<table>
<thead>
<tr>
<th>BUSINESS IMPACT</th>
<th>IMPACT OF DISRUPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HIGH</td>
</tr>
<tr>
<td>DATA LOSS</td>
<td></td>
</tr>
<tr>
<td>TIME SENSITIVITY</td>
<td></td>
</tr>
<tr>
<td>INTERACTIONS</td>
<td></td>
</tr>
</tbody>
</table>

**BUSINESS IMPACT**
What would be the impact in terms of loss of productivity, revenue or reputation if the applications/functions related to this project were not available or could not be performed?

**DATA LOSS**
What would be the impact of in terms of loss of productivity, revenue or reputation if key data were lost or unrecoverable?

**TIME SENSITIVITY**
What would be the maximum amount of time the function/application could be unavailable given the Business Impact identified above?
- High: 2 hours or less
- Medium: 2 – 48 hours
- Low: 48 hours or more

**INTERACTIONS**
What would be the impact if key business partners (internal/external) were unable to conduct their end of this process?
Resource Classification

The IT Application Owner is responsible for the completion of this section (depicted from Project Perspective)

4. RESOURCE IDENTIFICATION
Instructions: Indicate all the platforms required by checking as many boxes as apply. Specify the location for each platform. Check NEW to indicate that the project will require a new server or other addition to the technology infrastructure.

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>NEW</th>
<th>INTERNAL TO COMPANY</th>
<th>EXTERNAL TO COMPANY</th>
<th>SYSTEM BACKED UP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
<td>LOCATION(S)</td>
</tr>
<tr>
<td>Mainframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tandem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS400</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS6000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sun</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>(specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example Only
## Transaction Flow

The IT Application Owner is responsible for the completion of this section.

### 5. INTERFACES AND OTHER REQUIREMENTS

*Instructions: Check as many boxes as apply to indicate connectivity and transaction flow information.*

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>INTERNAL</th>
<th>EXTERNAL</th>
<th>DESCRIPTION</th>
<th>INTERNAL</th>
<th>EXTERNAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td></td>
<td></td>
<td>NDM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MQ</td>
<td></td>
<td></td>
<td>WOLF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web - JAVA</td>
<td></td>
<td></td>
<td>Web - ActiveContent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td></td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
<td>Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
<td>Other (specify)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
<td></td>
<td>Other (specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy Evolving

- Privacy expectations changing
- The “opt out” debacle
  - Consumer study
BREAK

- Please be back in

10 Minutes
Security Foundation
Start With Basics

**Reliability** the business need to have accurate, complete and timely information

**Confidentiality** the business need to maintain customer information, privacy, and corporate information confidentially

**AVAILABILITY** the business need to have information available when required

Consider: Authorized User Passwords remain the weakest link!
IT Security Components

- Security Architecture
- Network Security
- Security Operations
- Access Provisioning
- IT Risk Reporting & Compliance
Security Architecture

- End-to-End Requirements Analysis
- Risk Assessment Lead
- Pertinent technology research
- Active vendor interaction
- Pertinent Policies, Standards, Guidelines leadership
Network Security

- Vulnerability Management
- Network Perimeter Security
- Incident Response Leadership
Security Operations

- Authentication
- Cryptography
- Client Server Security
- Mainframe/Tandem Security
- Unix Security
  - Unix
  - NT
Access Provisioning

- Access Enablement
- ID Assignment & Password Reset
IT Risk Reporting & Compliance

- Compliance
- Monthly Status Reporting
- Outsourcing Relationship Tracking
- Awareness
- Audit/Log Reporting
- Human Resource Coordination
  - Related HR Policy Issues
    - The case of the “Porn King”
Some Leadership Points

- Tracking and reporting on progress
- "Security" (and Contingency Planning) are no longer a small budget item
- Senior IT security management must have skills to:
  - Develop business cases
  - Manage projects
  - Manage budgets
  - Present to Board Members
  - Proactively identify & take action on evolving issues
  - Participate & lead industry groups
Email – A Point on Security

- Don’t assume privacy
- You would be surprised at the business transactions done via email!
  - Lab results
  - Trade confirmations
  - Home mortgage loan and other financial account changes, inquiries, complaints, etc.
- Employee harassment via anonymous email
  - AN ACTUAL SET OF INCIDENTS (no details in handout)
- Now, let me introduce you to Andre Bacard…
Anonymous Remailer FAQ

Written by
André Bacard, Author of
Computer Privacy Handbook
[Updated 15 December 2002]

This FAQ, first published in 1995, offers a nontechnical overview of "remailers" to help you decide whether to use these computer services. When I first wrote this FAQ, remailers were an esoteric subject. Today, millions of persons use them. Links at Bacard's Privacy Page will connect you to specific remailers. I have written this FAQ for law abiding persons with a sense of irony. You may distribute this (unaltered) FAQ for non-commercial purposes. Thank you to the many pro-privacy sites around the world which link to this FAQ. Copyright 2002 by André Bacard.

What is a remailer?

A remailer is a computer service which privatizes your email. High-quality remailers are in sharp contrast to the average Internet Service Provider (ISP) which is terribly anti-private. In many cases, ISPs could accurately stand for "Internet Surveillance Project". Almost every ISP can monitor, store, and share your web wanderings and email with many "authorized persons" without your knowledge. In many countries ISPs are monitored constantly by government agencies.

In my opinion, all ISPs should be required by law to notify every customer:

"WARNING: Internet/Email Technology is the Most Comprehensive Surveillance System Ever Invented."

I urge everyone reading this FAQ to learn what this warning label means and to educate everyone who will listen to take necessary precautions.

Click here to Learn About Email Privacy.

Until the late 1990s, a remailer allowed you to send electronic mail to a Usenet news group, or to a person, without revealing your true name or email address to the recipient. Today, web-based remailers permit you to send email using your real name (if you wish), while protecting your email privacy.
until the late 1990s, a remailer allowed you to send electronic mail to a Usenet news group, or to a person, without revealing your true name or mail address to the recipient. Today, web-based remailers permit you to send email using your real name (if you wish), while protecting your email cords from the snooping eyes of your Internet Service Provider and others.

the first version of this FAQ (published in 1995), all popular remailers were free-of-charge. Today, a number of services either charge user fees, support themselves via advertisers.

why would YOU use remailers?

Maybe you're a computer engineer who wants to express opinions about computer products, opinions that your employer might hold against you. Possibly you live in a community that is violently intolerant of your social, political, or religious views. Perhaps you're seeking employment via the Internet and you don't want to jeopardize your present job. Possibly you want to place personal ads. Perchance you're a whistle blower afraid of retaliation. On the other hand, you might be an honest bureaucrat who invites whistle-blowers. Conceivably you feel that, if you criticize your verum, Big Brother will monitor you. Maybe you don't want people "spamming" or "flaming" your corporate email address. In short, there are many legitimate reasons why you, a law abiding person, might use remailers.

how does a remailer work?

It's take an elementary, imaginary example. Suppose that a battered woman, Susan, wants to post a message crying out for help. How can Susan post her message and receive responses confidentially? She might use a "PSEUDO anonymous" remailer run by André Bacard called the SecretBacard.com remailer. (This remailer is fictitious!) If she wrote to me, my "SecretBacard.com" computer would STRIP AWAY Susan's real name and address (the header at the top of Susan's email), replace this data with a dummy address (for example, anon123@SecretBacard.com) and forward Susan's message to the newsgroup or person of Susan's choice. Also, my computer would automatically notify Susan that her message had been forwarded under her new identity <anon123@SecretBacard.com>. Suppose that Debbie responds to Susan. My computer will STRIP AWAY Debbie's real name and address, give Debbie a new identity, and forward the message to Susan. This process protects everyone's privacy. This process is tedious for a person but easy for a computer.

are there many remailers?

Yes, there are dozens of popular remailers.
G-L-B-A Key Points
Gramm-Leach-Bliley-Act

- Public Law 106-102
- November 12, 1999
- Three Fundamental Financial Services Changes
  - Repeals key provisions of Glass Steagall Act permitting commercial banks to affiliate with investment banks
  - Substantially modifies the 43-year old Bank Holding Company Act of 1956 permitting companies that own commercial banks to expand services of financial activity
  - Allows bank subsidiaries to engage in broad range of financial activities that are not permitted for banks themselves
Gramm-Leach-Bliley-Act

- Other Important Provisions
  - Eliminates the authority of commercial companies to acquire thrift institutions through the unitary thrift holding company vehicle
  - New provisions regarding privacy of customer information
  - Increased access by community banks to the Federal Home Loan Bank System
  - Significantly changes the requirements imposed by the Community Reinvestment Act
G-L-B-A Key Effective Dates

- Title I – Affiliations
- Title II – Securities
- Title III – Insurance Regulation
- Title IV – Unitary Thrift Holding Companies
- Title V – Privacy
- Title VI – Federal Home Loan Bank System Reforms
- Title VII – Miscellaneous Regulatory Provisions
Focus G-L-B-A Discussion

- Title V – Privacy
  - Financial Institutions Must
    1. Establish and Annually Disclose Privacy Policy
    2. Provide consume right to prevent disclosure of nonpublic personal information to a nonaffiliated third party (“opt out”)
    3. Prohibits disclosure of account number, or equivalent thereof, for use in telemarketing
    4. Provision that “it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information”
Significant Issues

- Wording
  - “policy of the Congress”
- Effects of the privacy disclosures
- “Opt out” debacle
<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>August 21</td>
<td>Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) requiring the Secretary of Health &amp; Human Services to propose standards to protect the privacy of individually identifiable health information by August 21, 1997.</td>
</tr>
<tr>
<td>1997</td>
<td>September 11</td>
<td>U.S. Secretary of Health and Human Services (HHS) submitted a report to Congress recommending comprehensive privacy legislation by August 21, 1999. The Secretary was directed to finalize regulations containing proposed standards relating to electronic transfer of medical information by February 21, 2000 should congress fail to act by the proposed 1999 date.</td>
</tr>
<tr>
<td>1999</td>
<td>August 21</td>
<td>Congress was unable to reach consensus on comprehensive privacy legislation therefore the HHS Secretary took action to finalize related regulations.</td>
</tr>
<tr>
<td></td>
<td>October 29</td>
<td>The Clinton Administration announced the proposed rules.</td>
</tr>
<tr>
<td></td>
<td>November 3</td>
<td>Proposed privacy standards were published in the Federal Register for public comment.</td>
</tr>
<tr>
<td></td>
<td>August 17</td>
<td>Final Transaction and Code Sets Final Rule Published.</td>
</tr>
<tr>
<td></td>
<td>December 20</td>
<td>Final regulations and compliance deadline released by the HHS Secretary. Initial deadline was February 26, 2003 but was later extended to April 14, 2003.</td>
</tr>
<tr>
<td></td>
<td>December 28</td>
<td>Final Privacy Rule published in the Federal Register.</td>
</tr>
<tr>
<td>2001</td>
<td>July 6</td>
<td>HHS issued first guidance on privacy protections.</td>
</tr>
<tr>
<td></td>
<td>December 27</td>
<td>H.R. 3323, the Administrative Simplification Compliance Act (Public Law 107-105), signed in to law by President Bush. Provides 1 year compliance extension for compliance with standard transactions and code set requirements.</td>
</tr>
<tr>
<td>2002</td>
<td>March 27</td>
<td>Proposed changes to privacy standards published in the Federal Register.</td>
</tr>
<tr>
<td></td>
<td>October 16</td>
<td>Transaction and Code Set compliance deadline unless extension request filed/accepted by DHHS by 10/15/02.</td>
</tr>
<tr>
<td>2003</td>
<td>February 20</td>
<td>Final rule adopting standards for electronic PHI security published in the Federal Register.</td>
</tr>
<tr>
<td></td>
<td>April 14</td>
<td>Privacy standards compliance deadline for all covered entities except small health plans (less than $5M in annual receipts).</td>
</tr>
<tr>
<td></td>
<td>October 16</td>
<td>Compliance deadline for Transaction and Code Sets.</td>
</tr>
<tr>
<td>2004</td>
<td>April 14</td>
<td>Privacy standards compliance deadline for small health plans (less than $5M in annual receipts).</td>
</tr>
<tr>
<td></td>
<td>April 21</td>
<td>Electronic PHI Security Standards compliance deadline.</td>
</tr>
</tbody>
</table>
HIPAA

- Public Law 104-191
- August 21, 1996
- General Objectives
  - Assure health insurance portability by eliminating job-lock associated with pre-existing medical condition clauses
  - Reduce fraud by enhancing detection capabilities
  - Streamline paperwork through standardization
  - Guarantee security and privacy of health information
Other Concerns

- Identity Theft
- Terrorism
- Technology Controls
  - Implications, Capabilities, Limitations
- Operation Controls
- Operation/Technology control transition
- Business Process Engineering
Noteworthy

- Outsourcing
- MIS Test and QA Environments
- Consultants and their equipment
- Software vendor access to systems
  - Remote
  - On site
- External Auditors
  - Do they bring in their lap tops?
Enabling Implementation

1. Identify Information Owners
2. Identify pertinent data
   - Risk Assessment Process
3. Identify authorized access
   - Role-based Access Provisioning
4. Ensure proper documentation of transaction flow
5. Identify systems, applications, databases that store/process/transport (item 2)
Enabling Implementation

6. Identify control capability (operationally and technically) – perform gap analysis based upon requirements defined in Risk Assessment

7. Prepare business case and submit via proper channels

Note: Leadership is REQUIRED
What we have covered…

- Explore privacy issues from multiple perspectives
- Establish a mental framework to create solutions to reduce privacy exposures
- Understand technology-induced exposures to privacy
- Understand requirements as prescribed by the Gramm-Leach-Bliley Act 501(b)
- Understand requirements as prescribed by the Health Insurance Portability and Accountability Act of 1996
- Realize applicability to participants through hypothetical case studies
- Explore privacy matters from multiple perspectives:
  - Citizens
  - Business Leaders
  - Investors
Any Other Questions or Comments?

It has been a pleasure to meet with you. Thank you for your participation.

Sharon O’Bryan
skobryan@obbi.com
(630) 762-0801