

How Privacy Relates to Security

Privacy Symposium
Privacy Certificate Program Training

August 2008

Agenda

- ▶ Privacy and Security in Context
- ▶ Common Privacy Requirements for Security
- ▶ Traditional Information Security
- ▶ Common Gaps in Tradition



Privacy and Security in Context

Information Types

- ▶ Financial

- ▶ General ledger, accounts payable and receivable
- ▶ Financial reporting
- ▶ ...

- ▶ Human resources

- ▶ Performance management
- ▶ Compensation and benefits
- ▶ Talent management
- ▶ Succession planning
- ▶ Learning and development
- ▶ ...

- ▶ Operational

- ▶ Customer
- ▶ Supply chain
- ▶ Manufacturing
- ▶ Sales and marketing
- ▶ Service
- ▶ ...

- ▶ Intellectual property

- ▶ Trade secrets
- ▶ Plans, designs, and methods
- ▶ Secret recipes
- ▶ ...

- ▶ Information products

- ▶ ...

Privacy, Confidentiality, and Information Security

Privacy

- ▶ “Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.”
 - ▶ AICPA Generally Accepted Privacy Principles

Confidentiality

- ▶ “The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.”
 - ▶ ISO 27001:2005

Information Security


- ▶ “Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.”
 - ▶ ISO 27001:2005

Take Aways

Privacy relates to personal
information

Security and confidentiality can
relate to all information

Different information have different requirements for privacy, security,
and confidentiality



Common Privacy Requirements for Security

Safeguarding Personal Information

The organization shall protect personal information from unauthorized access, misuse, and denial of service using means that are:

- ▶ Commercially reasonable
- ▶ Aligned with best practices
- ▶ Reasonable
- ▶ Adequate
- ▶ Effective

The primary question is how much security is enough security?

GLBA-related Safeguards Rules

The Safeguards Rules require financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

- ▶ Designate one or more employees to coordinate the safeguards
- ▶ Identify and assess the risks to customer information in each relevant area of the Company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks
- ▶ Design and implement a safeguards program, and regularly monitor and test it
- ▶ Select appropriate service providers and contract with them to implement safeguards
- ▶ Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards

US Safe Harbor

Security

- ▶ Organizations creating, maintaining, using or disseminating personal information must take ***reasonable*** precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

California AB 1950

Code 1798.81.5 (a)

- ▶ A business that obtains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

EU Data Protection Directive

Confidentiality and Security (Articles 16 and 17)

Confidentiality

- ▶ Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Security

- ▶ The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
- ▶ The controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
- ▶ The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller.
- ▶ For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and shall be in writing or in another equivalent form.

UK Data Protection Act of 1998

Seventh Principle

- ▶ Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

FACTA Example of Specific Requirements

Truncation of Credit Card and Debit Card Numbers:

- ▶ In general, except as otherwise provided in this subsection, no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration data upon any receipt provided to the cardholder at the point of the sale or transaction.

This is a safeguard. It is not traditional “information security”. Who will make sure this happens?



Traditional Information Security

Information Security

Information security is the preservation of the confidentiality, integrity, and availability of information

“CIA”

- ▶ Confidentiality
 - ▶ Ensuring that information is accessible only to those authorized to have access
- ▶ Integrity
 - ▶ Safeguarding the accuracy and completeness of information and processing methods
- ▶ Availability
 - ▶ Ensuring that authorized users have access to information and associated assets when required

Basic Security Needs

In fact, security needs to be considered to a more detailed level.



Basic Security Needs

- ▶ To ensure the availability of information and services
- ▶ To securely allow access to information and services
- ▶ To prevent loss of integrity of information and transactions
- ▶ To provide authenticity of all parties involved
- ▶ To provide confidentiality of information and transactions
- ▶ To provide non-repudiation to all parties involved
- ▶ To provide an audit log of significant events
- ▶ To provide fraud prevention and other misuse controls

Key Security Principles

Separation or Segregation of Duties Need to Know/Need to Access

- ▶ Dividing responsibility for processing or information so that no individual acting alone can compromise the security

- ▶ The legitimate requirement of a person or organization to know, access, or possess specific information that is critical to the performance of an authorized, assigned mission. The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.

Least Privilege

- ▶ The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system

Standards for Information Security

ISO 27001: Information Security Management – Specification With Guidance for Use

- ▶ Common model for implementing and operating an Information Security Management System
- ▶ Comprehensive set of controls comprising best practices for information security management

ISO 17799/27002: Information Technology—Security Techniques—Code of Practice for Information Security Management

- ▶ Defines an overarching security framework consisting of 133 specific controls organized around 39 control objectives

Question: Is best practice reasonable, adequate, or effective?

Security Domains

The 11 security clauses of ISO 27002 each have categories of controls and implementation guidance for consideration.

Organizational

- 
- ▶ Security policy
 - ▶ Organization of information security
 - ▶ Asset management
 - ▶ Access control
 - ▶ Compliance
 - ▶ Human resources security
 - ▶ Physical and environmental security
 - ▶ Information systems acquisition, development and maintenance
 - ▶ Communications and operations management
 - ▶ Business continuity management
 - ▶ Information security incident management

Operational

A decorative graphic at the top of the slide. On the left, a series of vertical black lines of varying heights form a triangular shape pointing towards the center. On the right, a solid yellow triangle points towards the center, meeting the lines. The background is a light gray.

Common Gaps in the Tradition of Information Security

Common Gaps in Traditional Information Security

- ▶ Security programs have focused on corporate or other central systems and business functions, with limited impact on line of business systems
- ▶ Security programs have been focused on Sarbanes-Oxley §404 internal controls, and have ignored non-financial processes
- ▶ Data classification does not contemplate personal information in context
- ▶ Security programs are focused on IT, not accounting for security in the application and business process
- ▶ Business units do not know how to apply security policy and procedures inside of their business processes
- ▶ Portable devices and media containing personal information, and electronic transfer of personal information are not consistently protected
- ▶ Information security of third parties remains only hopeful, with little specific requirements, inconsistent legal protections, and little or no assurance
- ▶ Adequacy or reasonableness levels are not established

Closing the Gaps: Making It Adequate

- ▶ Deliberately extend the information security program to cover all systems and processes that handle personal information
- ▶ Differentiate information protection requirements for the various categories of personal information (and not by data element)
- ▶ Educate information security staff and management about the compliance requirements related to personal information so that policies and practices may be brought up to date
- ▶ Educate user of personal information about policies, but also give them enablers for security
- ▶ Provide active protection for portable devices, portable media, and electronic communications containing personal information
- ▶ Provide meaningful security requirements to third parties that are legally binding; develop an approach to gain the appropriate level of assurance over third party security
- ▶ Establish goals for adequacy and reasonableness of controls that includes tests of their effectiveness

Questions



Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

About Ernst & Young's Technology Risk and Security Services

Information technology is one of the key enablers for modern organizations to compete. It gives the opportunity to get closer, more focused and faster in responding to customers, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and security issue. And because we understand that, to achieve your potential, you need a tailored service as much as consistent methodologies, we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information, please visit www.ey.com.

© 2008 EYGM Limited. All Rights Reserved.

Proprietary and confidential. Do not distribute without written permission.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.
