IAPP Privacy Certification

Certified Information Privacy Professional

Information Security

Robert Jervay
Partner

Deloitte.

agenda

- definitions
- information infrastructure
- the IT organization
- information asset oversight

agenda

- information systems access
- contingency planning
- incident handling

definitions

definitions

Information Security

"You can have security without privacy, but you cannot have privacy without security"

Information Security is the protection of information to prevent loss, unauthorized access or misuse. It is also the process of assessing threats and risks to information and the procedures and controls to preserve:

- Confidentiality: Access to data is limited to authorized entities
- Integrity: Assurance that the data is accurate and complete
- Availability: Data is accessible, when required, by those who are authorized to access it

definitions

Security Controls

Security controls are the set of organizational structures, policies, standards, procedures, and technologies which support the business functions of the enterprise while reducing risk exposure and protecting information

- Preventative: Designed to keep errors or irregularities from occurring
- Detective: Designed to detect errors and irregularities which have already occurred and to report to appropriate personnel
- Responsive: Designed to respond to errors or irregularities to restore operations and prevent future issues
- Administrative: Processes and procedures
- Technical: Software and hardware technologies
- Physical: Facility and environmental security

information infrastructure

information infrastructure

Data Management

Security protection of personal information starts with strong data management practices

- **Database Management**
  - User access controls
  - Database administrator access controls
  - Restrictions on view, update, modification, or deletion of data
  - Appropriate usage guidelines for data
  - Use of real personal information in development and test environments
- **Backups**
  - Backup media should be secure
  - Backups should be reliable for recovery purposes
  - Backup and restore processes should be controlled to avoid errors and unauthorized access
  - Backup media should be tested regularly to ensure integrity
- **Recovery**
  - Recovery plans should be documented and tested
  - Data recovery is usually integrated with disaster recovery and business continuity plans

information infrastructure

Hardware

Know where personal information resides within your organization and how to protect the repositories

- **Mainframe / Servers / Storage Systems**
  - Large, computing hardware installations, generally housed within a defined building area with good physical security
  - Usually have defined security processes and controls
  - Access is typically controlled and data may be classified
- **Desktops / Laptops / Handheld Devices**
  - Each of these computing platforms provides additional challenges for security and privacy as both functionality increases and control decreases
  - Personal information stored on local systems is an issue due to greater exposure and lack of appropriate backups
  - Personal information on laptops and handhelds presents additional concerns due to portability
  - Hardware theft is a common occurrence, and some have specifically targeted the data stored on them
  - Encryption technologies can be utilized to lower risk exposure
- **Media / Mass Storage Devices**
  - Increasing capacity and availability
  - Difficult to track location
  - Easy to steal and lose

information infrastructure

Networks

Networks allow for communication between systems and people, but introduce significant challenges from a privacy and security perspective

- **Local Area Networks (LANs)**
  - **Within the operational facility**
  - **Considered within local operational control and easier to manage**
- **Wide Area Network (WANs)**
  - **Considered outside of local operational controls and are more difficult to manage**
  - **May involve coordination between several groups**
- **Internet**
  - **Public resource used and accessed by anyone**
  - **Generally considered untrusted and requires additional network security controls such as encryption**
- **Network Topologies**
  - **Ethernet**
  - **Optical**
  - **Wireless**

information infrastructure

Networks

Remote Access

- Provides connectivity with employees and partners from outside of local operational control
- Requires additional measures such as access controls

Mobile and Wireless Networks

- Susceptible to eavesdropping and unauthorized access
- Use caution and implement encryption where possible

Telecom – Voice over Internet Protocol (VoIP)

- Utilizes Internet and WAN connectivity
- Susceptible to Internet attacks

Broadband

- Always on, high bandwidth connections often targeted by attackers
- Digital Subscriber Line (DSL) – Dedicated connection to Internet
- Cable Internet – Local network shared with other users

Virtual Private Networks (VPN)

- Uses encryption technology to set up private connections across public networks
- Adds layer of security to communications

information infrastructure

Internet

Sharing and accessing personal information over the Internet requires special controls

- **Web-Based Applications**
  - Accessible from anywhere in the world, hence open to attacks from anywhere
  - Transfers of personal information should be encrypted using SSL
- **E-Commerce**
  - Online commercial transactions require personal financial information to be exchanged
  - Transmission and storage of financial information poses additional risks with the rise of identity theft
- **E-Business**
  - Transmission of personal information as part of e-business transactions is common
  - Data sharing between business partners via e-business channels should follow the same procedures and controls as other data sharing mechanisms

Email

The ubiquitous and ad hoc nature of email communications makes personal information difficult to protect

- Information sent in email can be intercepted, read and manipulated unless there is network or application level encryption
- Standard email communication sent outside of the business is analogous to sending a postcard (unless encrypted)
- Information transmitted via email is no longer under your control
- Email phishing schemes to steal personal information are on the rise

the IT organization

Information Technology Management

Good information security starts with sound information technology management practices

- Information technology and information security should be formal, budgeted functions, supporting the business operation
- Information security must be included in the business life cycle from design through retirement
- Information technology infrastructure must be built to include information security through all interfaced systems
- Project management must be formalized and include change management and security controls
- Outsourcing must include security controls and be managed internally to ensure protection of personally identifiable information

the IT organization

Roles & Responsibilities

To maintain security within the organization, roles and responsibilities must be clearly understood

- **Chief Executive Officer & Executive Committee**
  - Oversee overall corporate security strategy
  - Lead by example and sponsor adoption of security
- **Chief Security Officer**
  - Sets security strategy and policies
  - Facilitates the implementation of security controls
  - Undertakes security risk assessments
  - Designs risk management strategy
  - Coordinates independent audits
- **Security Personnel**
  - Implement, audit, enforce, & assess compliance
  - Advise and validate security designs and maintenance
  - Keep abreast of new security developments (vulnerabilities, exploits, patches)
  - Communicate policies, programs & training
  - Monitor for security incidents
  - Respond to security breaches
- **Outsourced Security Functions**
  - Supplements internal security personnel
  - Should be overseen by internal security personnel
- **Managers & Employees**
  - Implement security controls
  - Report security vulnerabilities and breaches
  - Maintain awareness of security in action

Outsourced Activities

The security requirements of an organization engaging in outsourcing should be addressed in a contract agreed upon between the parties

It should reflect:

- Security roles and responsibilities
- Requirements for data protection to achieve comparable levels of security
- Data ownership and appropriate use
- Physical and logical access controls
- Security control testing of the service provider
- Continuity of services in the event of disaster
- Incident coordination process
- Right to conduct audits
- Respective liabilities

Security Awareness Training

Technology alone cannot provide information security – education and awareness of personnel is key

Ensure that all employees understand:

- The value of security and are trained to recognize and report incidents
- Their roles and responsibilities in fulfilling their security responsibilities
- Security policies and procedures, including password protection, data sensitivity, information protection
- Basic security issues such as virus, hacking, and social engineering
- The importance of compliance with regulatory requirements such as HIPAA, Sarbanes-Oxley and Gramm-Leach-Bliley

information asset oversight

information asset oversight

Asset Management

To effectively manage information security, an organization must understand which data assets are critical to the function of the company

- **Locate and identify the information to be protected**
  - **Develop tracking for data assets and the systems which house them**
- **Differentiate between owned vs. used assets**
  - **Owners create and change**
  - **Users access and execute**
- **Record Retention**
  - **Retention schedules should address record types and retention periods**
  - **Retention should be based on business need or regulatory requirement**
  - **Inventories of key information should be maintained**
  - **Controls should be implemented to protect essential records and information from loss, destruction and falsification**

information asset oversight

Asset Classification Criteria

Data should be protected in accordance with the value of the asset—the higher the value, the greater the security needed

- Value should be evaluated based on:
  - Sensitivity
  - Confidentiality
  - Potential liability
  - Intelligence value
  - Criticality
- Effective risk management balances the potential for loss with cost of security protection and management

information asset oversight

Data Classification

A data classification scheme, like the one in the example below, provides the basis for managing access to and protection of data assets

- **Confidential**
  - Data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations
  - Examples of this data type are social security numbers and credit card numbers
- **Proprietary**
  - Data whose loss, corruption or unauthorized disclosure would tend to impair the function of the business, or result in any business, financial, or legal loss
  - Examples of this data type could be customer financial records
- **Internal Use Only**
  - Data whose audience is intended to be those who work within the organization
  - Examples of this data type could be phone lists or email distribution lists
- **Public**
  - Data whose audience may include the general public
  - Examples of this data type could be press releases or marketing materials
- **Additional Classification Types**
  - Depending on the amount and types of data collected by the organization, additional classifications may be advised due to current regulatory requirements

information systems security

information systems security

Authentication

Authentication identifies an individual based on some credential (e.g., password, smartcard, biometric)

- **Identification of the individual**
  - Individual account requirement
  - Separate administration and user accounts
  - No anonymous or shared accounts for access to personal information
  - Special care for system accounts
- **Passwords**
  - Encryption in transfer and storage
  - Complexity requirements
  - Change frequency requirements
  - Repetition restrictions
  - Storage guidelines
  - No-sharing policy
  - Disabling on change, termination or departure
- **Non-repudiation**
  - The ability to ensure that neither the originator nor the receiver can dispute the validity of a transaction
- **Public key infrastructure (PKI)**
  - System of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction using cryptography

Authorization

Authorization is the process of determining if the user, once identified, is permitted to have access to the resource and may be based on:

- Organizational role
- Job function
- Group membership
- Level of security clearance
- Purchased access

information systems security

Access

Access defines the intersection of identity and data; that is, who can do what to which data

- Role-based: need to know / have
  - Based on the principle of the least possible access required to perform the function
  - Periodic review of accounts and access rights
  - Deletion or termination of access based on work or position changes
  - Periodic review of idle accounts
- Workstation locking mechanisms
  - Password-protected screen savers
  - Time-activated lockouts
- Access policy for email, Internet and portable devices
- Identity management solutions
  - Authoritative source
  - Single or reduced sign-on
  - Segregation of duties
  - Ease of access with controls

Intrusion Prevention

- Prevention is the best possible cure
- Firewalls
- Anti-virus
- Content scanning
- Security patches
- Emerging intrusion prevention systems
- User awareness

contingency planning

contingency planning

Threats and Vulnerabilities

Risk is a function of the likelihood of a threat exploiting a security vulnerability with a resulting impact

- **Potential threats**
  - Emergency situations or natural events
  - Organized or deliberate malicious actions
  - Internal accidents, carelessness, or ignorance
  - Malicious code (virus, worms, spyware, malware)
  - Loss of utilities or services
  - Equipment or systems failure
  - Serious information security events
- **Security vulnerabilities**
  - Unsecured accounts
  - Unpatched systems
  - Insecure configurations
  - Network perimeter weaknesses
  - Inappropriate trust models
  - Untrained users and administrators

Disaster Recovery

The disaster recovery plan allows an organization to respond to an interruption in services by implementing a disaster recovery plan to restore critical business functions and data

- Disaster recovery plan
  - Conditions for activating
  - Emergency procedures
  - Fallback procedures
  - Resumption procedures
  - Roles and responsibilities
  - Awareness and education
  - Maintenance schedule
- Backups
  - Systems, applications and information
  - Cold, warm or hot sites
  - Redundant or recoverable
  - Secure and reliable

contingency planning

Business Continuance

The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before, after, and during an event

- **Business continuity plan**
  - **Business process recovery**
  - **Human resource management**
  - **Facilities availability**
  - **Information systems recovery**
  - **Customer service restoration**
  - **External business partner functions**

incident handling

incident handling

Incident Response

Indications of an incident

- Failed login
- Dormant account login
- Nonwork-hour activity
- Presence of new accounts (unknown)
- System log gaps
- Unfamiliar programs or files
- Unexplained elevation of user privileges
- Unexplained change in file permissions
- Unexpected malfunction or error message
- System failures

Early alerts from multiple sources

- User community
- System administration staff
- Security team
- Intrusion detection systems
- Vendors & security companies

Formal incident response plans

- Identification
- Communications
- Containment
- Backup
- Recovery
- Post-mortem

incident handling

Incident Documentation

Forensic evidence

- Admissibility of evidence
- Quality of evidence
- Preservation of integrity

Post-mortem

- Document incident, response activities, and results
- Gather lessons learned
- Measure metrics such as type, frequency, cost
- Monitor for trends
- Incorporate into future security controls design

conclusion

incident handling

Information Security Training

- Definitions
- Information Infrastructure
- The IT Organization
- Information Asset Oversight
- Information Systems Security
- Contingency Planning
- Incident Handling

Question & Answer Session

IAPP Certification Promoting Privacy