Regulations and Compliance

CPSC 4670 @ UTC

Motivation

- Regulators have created a large and growing set of regulations and frameworks aimed at enforcing protection of information, privacy, and transparency of information.
- For example, HIPAA for healthcare, GLBA for financial services, and Sarbanes-Oxley for public companies.

Motivation

- Questionable accounting practices and poor management in companies such as Enron and Worldcom shattered investor confidence and caused Congress to pass Sarbanes-Oxley Act of 2002 (SOX)
- To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities law.
- All of these systems employ relational databases, and these projects include database security and auditing implementations.

Gramm-Leach-Bliley Act (GLBA)

- Also called Financial Services Modernization Act or Citigroup Relief Act.
- Enacted 7 months after the merger between Citicorp and Travelers Group to form CitiGroup.
- Applied to financial holding company (FHC)
- It allows FHC like CitiGroup to own banks, insurance and securities firms.
- One of main reasons for creating mega-financial companies is to leverage a knowledge base and be able to do cross-selling within the FHC.
- insurance company can market products to customers of the bank if they are in one FHC.
- Individual privacy may be risky.

Gramm-Leach-Bliley Act (GLBA)

- To combat extreme misuse of such cross-selling and the risks to privacy, Congress adopted Title V of GLBA, which defines various requirements designed to protect the privacy of customers financial institution.
- Title V includes both
  - the Financial Privacy Rule discussing operations and practices
  - The safeguard rule with more technical interpretation
    - Ensure the security and privacy of customer information
    - Protect against threats to the security and integrity of customer information
    - Protect against unauthorized access and/or usage of this information that could result in harm or inconvenience to the customer

Sarbanes-Oxley Act of 2002 (SOX or SarBox)

- Applied to public company with over $75 Million revenue
- SOA addresses many areas that affect the accuracy and transparency of financial reporting.
  - enforces accountability for financial record keeping and reporting at publicly traded corporations
  - Requires that CEO and chief financial officer (CFO) assume direct and personal accountability for completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems

Sarbanes-Oxley Act of 2002 (SOX or SarBox)

- As these executives attempt to ensure that the systems used to record and report are sound—often relying upon the expertise of CIOs and CISOs to do so—the related areas of availability and confidentiality are also emphasized
- IT people focus on Section 404, which requires management to report on the effectiveness of the company's internal control over financial reporting.

Sarbanes-Oxley Act of 2002 (SOX or SarBox)

- It requires management’s development and monitoring of procedures and controls for making assertions about the Adequacy of internal controls over financial reporting.
- It is management’s responsibility and can not be delegated or abdicated.
- Document and evaluate the design and operation of its internal control.

California Senate Bill 1386 (2003)

- Any business that maintains personal information of a resident of California must have the appropriate provisions and capabilities to know when this information may have been accessed by an unauthorized person.
- Focus on privacy, not just the need for privacy but the need for effective controls that will allow one to know when access controls has been compromised and data has been access in an unauthorized manner.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Objective
  - Guarantee health insurance coverage of employees
  - Reduce health care fraud and abuse
  - Protect the health information of individuals against access without consent or authorization

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Based on 164.520 – Notice of privacy practices for protected health information, providers must provide individuals with a notice of privacy practices in plain language.
  - Information about uses and disclosures of protected health information
  - An explanation of privacy rights
  - How to file complaints
- The providers have to give it to you and ask you to sign it, but you do not have to sign the document.

Health Insurance Portability and Accountability Act of 196 (HIPAA)

- Security requirement outlined in HIPAA require the following:
  - Management involvement in the development and implementation of HIPAA-compliant security policies and procedures
  - Periodic reviews of these policies and procedures
  - Training on policies and procedures for all employees who come in contact with private patient information
  - Technical measures that are integrated into the organizations' information systems

HIPPA: two types of confidential electronic information

- **ePHI = Electronic Protected Health Information**
  - Medical record number, account number or SSN
  - Patient demographic data, e.g., address, date of birth, date of death, sex, e-mail / web address
  - Dates of service, e.g., date of admission, discharge
  - Medical records, reports, test results, appointment dates
- **PII = Personally Identified Information**
  - Individual's name + SSN number + Driver's License # and financial credit card account numbers

HIPPA: Definition of "ePHI"

- **ePHI** or electronic Protected Health Information is patient health information which is **computer based**, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.
- **Electronic media** includes computers, laptops, disks, memory stick, PDAs, servers, networks, dial-modems, E-Mail, web-sites, etc.
  - **Federal Laws:** HIPAA Privacy & Security Laws mandate protection and safeguards for access, use and disclosure of PHI and/or ePHI with sanctions for violations.

HIPPA: Definition of "PII"

- **"Personal information"** – **Unencrypted computerized information** that includes an individual's name in combination with any one or more of the following: Social Security Number, Driver's license number, or California ID card #, credit / debit in combination with their access / security code or password
  - **State Law:** SB-1386 California, Privacy of Personal Information to Prevent Identity Theft. SB-1386 requires mandatory notice to the subject of an unauthorized, unencrypted electronic disclosure of "personal information".

HIPPA: What are the Information Security Standards for Protection of ePHI?

- “Information Security” means to ensure the confidentiality, integrity, and availability of information through safeguards.
- **“Confidentiality”** – that information will not be disclosed to unauthorized individuals or processes [164.304]
- **“Integrity”** – the condition of data or information that has not been altered or destroyed in an unauthorized manner. Data from one system is consistently and accurately transferred to other systems.
- **“Availability”** – the data or information is accessible and useable upon demand by an authorized person.

HIPPA: What are the Federal Security Rule - General Requirements? [45 CFR #164.306-a]

- Ensure the “**CIA**” (confidentiality, integrity and availability) of all electronic protected health information (**ePHI**) that the **covered entity** creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI, e.g., hackers, virus, data back-ups
- Protect against unauthorized disclosures
- Train workforce members (“awareness of good computing practices”)

Compliance required by April 20, 2005

HIPPA: Who is a “Covered Entity”?

- **HIPAA's regulations directly cover three basic groups of individual or corporate entities: health care providers, health plans, and health care clearinghouses.**
  - Health Care Provider means a provider of medical or health services, and entities who furnishes, bills, or is paid for health care in the normal course of business
  - Health Plan means any individual or group that provides or pays for the cost of medical care, including employee benefit plans
  - Healthcare Clearinghouse means an entity that either processes or facilitates the processing of health information, e.g., billing service, re-pricing company

HIPPA:"Isn't this just an I.T. Problem?"

Good Security Standards follow the "90 / 10" Rule:

- **10% of security safeguards are technical**
- **90% of security safeguards rely on the computer user to adhere to good computing practices**
  - Example: The lock on the door is the 10%. remembering to lock, ensuring others do not prop the door open, and keeping controls of keys is the 90%. 10% security is worthless without USER!

HIPPA: What are the Consequences for Security Violations?

- Risk to integrity of confidential information, e.g., data corruption, destruction, unavailability of patient information in an emergency
- Risk to security of personal information, e.g., identity theft
- Loss of valuable business information
- Loss of confidentiality, integrity & availability of data (and time) due to poor or untested disaster data recovery plan
- Embarrassment, bad publicity, media coverage, news reports
- Loss of patients' trust, employee trust and public trust
- Costly reporting requirements for SB-1386 issues
- Internal disciplinary action(s), termination of employment
- Penalties, prosecution and potential for sanctions / lawsuits

Payment Card Industry Data Security Standard

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications

Payment Card Industry Data Security Standard

Control Objectives	PCI DSS Requirements
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

More resources on PCI

- PCI Security Standards Council: https://www.pcisecuritystandards.org/index.shtml
- PCI and Oracle DB http://www.oracle.com/technology/deploy/security/database-security/oracle-pci.html

Understand Business needs and map to technical requirements

- Regulations and other privacy requirements do not typically define precisely what types of technologies need to be implemented.
- You will often be asked to suggest a set of concrete implementation options to bring your organization into compliance with these regulations.
  - Comply with regulations
  - Is implementable with reasonable cost

Use Reverse Mapping

- Start out with a list of security and auditing provisions that you have implemented, are implementing, or plan to implement.
- Check off items in the regulations that these security best practices cover.
- Couple that with auditing implementations.
- For example
  - Implement user-based and role-based privileges in your database, you may also have some context-related mechanisms. Section 142.308 requires one of three access controls: user-based, role-based, and context-based
  - Role-based access requires identification of the person or class of person. This maps to authentication and identification.

Timetable, data, and process mappings

- Make sure that the implementation phases and timetables map to the regulation timetables.
- Retention period, for example, HIPAA mandates a retention period of six years.
- Data mapping: identify the data in the database that maps to the information that the regulations discuss.

Example: SOX and Excel

- **Excel and other spreadsheets** have become the focus of many SOX implementations, because spreadsheets are extensively used in financial reporting and form the user interface layer in many financial application.
- Possible techniques
  - Monitoring source programs will give you a clear indication of which applications are accessing the database.
  - Baseline accessing will allow you to identify any divergence from normal access as a result of operations initiated using Excel and can help with an additional control and audit point in the spreadsheet macro’s change control process.

The role of auditing

- Audit as a function needs to play a central role in ensuring compliance. It includes
- Audit trails and other logs (auditing information)
- Security audits: assessments, penetration tests, or vulnerability scans, and focus on the current state of a database environment rather than auditing data.
- SQL Server Best Practices Analyzer Tool include and package a set of best practices, known vulnerabilities, and items that map well to compliance requirements.
- Continuous assessment evaluates potential flaws in the database environment – not in how it is configured but how it is used.
- Auditing is an integral part of security. There is no security without audit.

The importance of segregation of duties

- All regulations try to deal with a set of human behaviors such as untruthfulness, greedy, sloppiness, laziness, and so forth.
- Regulations use two main techniques: (1) guidelines so that people cannot too loosely interpret the regulations to their benefit and (2) segregation of duties.
- You can not trust the process to a single individual or a single group but need to build the process in a way so that you have multiple layers of audit.
- Auditing should be defined and performed by people other than those who work within the database every day.

Implement a sustainable solution

- You need to use tools that will do most of the work for you.
- You need to be able to get information at multiple levels.
- You must implement a solution that will sustain change.
- The solution should be well-packaged and self-maintaining.

"Good Computing Practices"
10 Safeguards for Users

1. **User ID** or Log-In Name (aka. User Access Controls)
2. **Passwords**
3. **Workstation Security**
4. **Portable Device Security**
5. **Data Management**, e.g., back-up, archive, restore.
6. **Remote Access**
7. **Recycling Electronic Media & Computers**
8. **E-Mail**
9. **Safe Internet Use**
10. **Reporting Security Incidents / Breach**

Safeguard - #1: Unique User Log-In / User Access Controls

- Access Controls:
  - Users are assigned a unique "User ID" for log-in purposes
  - Each individual user's access to ePHI system(s) is appropriate and authorized
  - Access is "role-based", e.g., **access is limited to the minimum information needed to do your job**
  - Unauthorized access to ePHI by former employees is prevented by terminating access
  - User access to information systems is logged and audited for inappropriate access or use.

Safeguard-#2: Password Protection

Passwords will be assigned to you for most data systems to comply with the security rule, but when necessary here are guidelines for choosing a password:

- Don't use a word that can easily be found in a dictionary — English or otherwise.
- Use at least eight characters (letters, numbers, symbols)
- Don't share your password — protect it the same as you would the key to your residence. After all, it is a "key" to your identity.
- Don't let your Web browser remember your passwords. Public or shared computers allow others access to your password.

Safeguard-#3: Workstation Security – Physical Security

- **"Workstations"** include any electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions.
- **Physical Security measures include:**
  - Disaster Controls
    - Protect workstations from natural and environmental hazards, such as heat, liquids, water leaks and flooding, disruption of power, conditions exceeding equipment limits.
  - Device & Media Controls:
    - Auto Log-Off or Automatic Screen Savers

Safeguard-#4: Security for Portable Devices & Laptops with ePHI

- **Implement the workstation physical security measures listed in Safeguard #3, including this Check List:**
  - Use an Internet Firewall
  - Use up-to-date Anti-virus software
  - Install computer software updates, e.g., Microsoft patches
  - Encrypt and password protect portable devices, e.g. USB memory stick
  - Lock-it up!, e.g., Lock office or file cabinet, cable
  - Automatic log-off from programs is possible
  - Use password protected screen savers
  - Back-up critical data and software programs
  - De-identify ePHI or delete ePHI from memory stick or PDA
  - Disable wireless or use VPN

Safeguard-#5: Data Management & Security

- Data backup and storage
  - Backup original data files with ePHI and other essential data and software programs frequently based on data criticality, e.g., daily, weekly, monthly.
  - Consider encrypting back-up disks
  - Permanent copies of ePHI should not be stored for archival purposes on portable device, such as laptop computers, PDAs and memory sticks.
  - If necessary, temporary copies could be used on portable devices, only when:
    - The storage is limited to the duration of the necessary use; **and**
    - If protective measures, such as encryption, are used to safeguard the confidentiality, integrity and availability of the data in the event of theft or loss.
- Transferring and downloading data
  - Encryption is an important tool for protection of ePHI in transit across unsecured networks and communication systems
- Data disposal
  - Destroy EPHI data which is no longer needed (professional overwrite)

Safeguard-#6: Remote Access

- Need consider authentication such as Radius
- Can adopt Virtual Private Network to encrypt communication in transit
- Use access control to authorize users
- Audit behavior of remote users

Safeguard-#7: E-Mail Security

Email is like a "postcard". Email may potentially be viewed in transit by many individuals, since it may pass through several switches enroute to its final destination or never arrive at all! Although the risks to a single piece of email are small given the volume of email traffic, **emails containing ePHI need a higher level of security.**

7-1 Should You Open the E-mail Attachment?

If it's suspicious, don't open it!

What is suspicious?

- Not work-related
- Attachments not expected
- Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, or *.pif)
- Web link
- Unusual topic lines; "Your car?"; "Oh!" ; "Nice Pic!"; "Family Update!"; "Very Funny!"

7-2. E-Mail Security – Risk Areas

1. **Spamming.** Unsolicited bulk e-mail, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
   - Do not reply to spam messages. Do not spread spam. Remember, sending chain letters is against UC policy.
   - Do not forward chain letters. It's the same as spamming!
   - Do not open or reply to suspicious e-mails.
2. **Phishing Scams.** E-Mail pretending to be from trusted names, such as Citibank or Paypal or Amazon, but directing recipients to rogue sites. A reputable company will never ask you to send your password through e-mail.
3. **Spyware.** Spyware is adware which can slow computer processing down; hijack web browsers; spy on key strokes and cripple computers

7-3. Instant Messaging (IM) - Risks

- **Instant messaging (IM) and Instant Relay Chat (IRC) or chat rooms create ways to communicate or chat in “real-time” over the Internet.**
- **Exercise extreme caution when using Instant Messaging on UC Computers:**
  - Maintain up-to-date virus protection and firewalls, since IM may leave networks vulnerable to viruses, spam and open to attackers / hackers.
  - Do not reveal personal details while in a Chat Room
  - Be aware that this area of the Internet is not private and subject to scrutiny

Safeguard-#8: Internet Use

- **Be careful about providing personal, sensitive or confidential information to an Internet site or to web-based surveys that are not from trusted sources.**
- Personal information posted to web-pages may not be protected from unauthorized use.
- Even unlinked web pages can be found by search engines
- Some web sites try to place small files ("cookies") on your computer that might help others track the web pages you access

Remember: **The Internet is not private!** Access to any site on the Internet could be traced to your name and location.

Safeguard-#9: Report Security Incidents

- **Users are responsible to:**
  - Report and respond to security incidents and security breaches.
  - Know what to do in the event of a security breach or incident related to ePHI and/or Personal Information.
- **Security Incident defined:**
  - "The attempted or successful improper instance of unauthorized access to, or use of information, or mis-use of information, disclosure, modification, or destruction of information or interference with system operations in an information system.“ [45 CFR 164.304]

Safeguard-#10: User Responsibility to Adhere to Information Security Policies

- CIO or CISO may use the following language in their trainings
- "Users of electronic information resources are responsible for complying with all policies, procedures and standards relating to information security."
- "Workforce members who violate policies regarding privacy / security of confidential, restricted and/or protected health information or ePHI are subject to further corrective and disciplinary actions according to existing policies."
- "Actions taken could include:
  - **Termination of employment**
  - **Possible further legal action**
  - **Violation of local, State and Federal laws may carry additional consequences of prosecution under the law, costs of litigation, payment of damages, (or both); or all.**
  - **Knowing, malicious intent → Penalties, fines, jail!"**

statistical database

statistical database

- A **statistical database** is a database used for statistical analysis purposes.
- Statistical databases often incorporate support for advanced statistical analysis techniques, such as correlations, which go beyond SQL.
- They also pose unique security concerns, which were the focus of much research, particularly in the late 1970s and early to mid 1980s.

Securing statistical database is difficult

- In a statistical database, it is often desired to allow query access only to aggregate data, not individual records.
- However, securing such a database is a difficult problem, since intelligent users can use a combination of aggregate queries to derive information about a single individual.

Common Approaches to Secure Statistical Database

Some common approaches are:

- only allowing aggregate queries (SUM, COUNT, AVG, STDEV, etc.)
- rather than returning exact values for sensitive data like income, only return which partition it belongs to (e.g. 35k-40k)
- return imprecise counts (e.g. rather than 141 records met query, only indicate 130-150 records met it.)
- don't allow overly selective WHERE clauses
- audit all users queries, so users using system incorrectly can be investigated
- use intelligent agents to detect automatically inappropriate system use

Mission Impossible?

- in general, securing statistical databases was an impossible aim:
  - if they were open to legitimate use, they were also open to abuse; and
  - if they were restricted so tightly as to be incapable of abuse, they would then be useless for practical statistical purposes.
  - statistical databases are almost always subject to compromise.
  - Severe restrictions on allowable query set sizes will render the database useless as a source of statistical information but will not secure the confidential records.

References

- doi:10.1145/320613.320616 - Dorothy E. Denning, Secure statistical databases with random sample queries, ACM Transactions on Database Systems (TODS), Volume 5, Issue 3 (September 1980), Pages: 291 - 315
- doi:10.1145/319830.319834 - Wiebren de Jonge, Compromising statistical databases responding to queries about means, ACM Transactions on Database Systems, Volume 8, Issue 1 (March 1983), Pages: 60 - 80
- doi:10.1145/320128.320138 - Dorothy E. Denning, Jan Schlörer, A fast procedure for finding a tracker in a statistical database, ACM Transactions on Database Systems, Volume 5, Issue 1 (March 1980) . Pages: 88 - 102
- Information is from wikipedia