NKU SALMON P. CHASE COLLEGE OF LAW
NORTHERN KENTUCKY UNIVERSITY

Current Trends in Computer Security

Duty, Breach,
Causation + Damage -

Think Torts to Stop Cyber Crimes

Professor Jon M. Garon
NKU Chase College of Law
Law + Informatics Institute

Coverage of Information

- The ultimate concern is electronic corporate information
- But protecting electronic information also requires addressing the means by which such information is created, stored, and communicated.
- Thus, statutes and regulations governing information security typically focus on the protection of both *information systems*
  - *computer* systems, networks, and software
  - *data, messages, and information* recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems
- If data were **wine**,
  - Protect the grapes and the field from physical intrusion and disease
    - One diseased grape can destroy an entire season
  - Protect the processing of the wine; the storage of the wine
  - Manage the access and distribution as well as the personnel

Duty - The law is everywhere

- **Compelled disclosure to the government**
  - Electronic Communications Privacy Act (ECPA)
  - Stored Communications Act (SCA)
  - USA Patriot Act (including National Security Letters; FISA warrants)
  - Warrants and Subpoenas Generally
- **Data security issues and data breach notification**
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Information Technology for Economic and Clinical Health Act and Health Insurance Portability and Accountability Act (collectively HIPAA)
  - Sarbanes Oxley (through guidance and guidelines)
  - Federal Information Security Management Act (FISMA) to promote
  - the security of federal agency information systems
  - Children's Online Privacy Protection Act (COPPA)
  - Family Educational Rights and Privacy Act (FERPA)
  - State Laws and Regulations
  - Section 5 of the FTC Act (for companies who will store consumer information on the cloud)
- **Access**
  - Americans with Disabilities Act

- Source: hoganlovels.com; Cisco

Gramm-Leach-Bliley Act Financial Privacy

- GLBA privacy considerations affect consumers in the following ways:
- Financial institutions are required to provide you with a notice of their information sharing policies when you first become a customer, and annually thereafter.
- Financial institutions are required to:
  - ensure the security and confidentiality of customer information;
  - protect against any anticipated threats or hazards to the security or integrity of such information; and
  - protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.
- The law requires these institutions to explain how they use and share your personal information. The law also allow you to stop or "opt out" of information sharing to unaffiliated third parties.
- Credit card numbers, pins or other access codes can no longer be sold.

GLBA Safeguards Rule

- The objectives of the GLBA Safeguards Rule are to:
- Insure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

- The Rule is intended to establish standards for financial institutions to develop, implement and maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
- The Rule covers any financial institution that is handling "customer information" - *i.e., not only financial* institutions that collect nonpublic personal information from their own customers, but also financial institutions that receive customer information from other financial institutions.

GLBA Safeguards Rule

- "This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you."
  - The duty applies, therefore to all business associates and other parties holding NPI
- Covers information "whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates."

- Five components:
  1. Designate employee responsible (and Board member or committee)
  2. Assess risks
  3. Design and implement safeguards
  4. Oversee service providers
  5. Evaluate, audit, adjust and redeploy continually

Employee/Insider Risk

- Stephen Wu: "Administrative safeguards are the non-technical, "soft" measures that management establishes regarding acceptable employee conduct, personnel procedures, and correct technology usage within the enterprise."
- "Companies should train and supervise their employees to prevent them from violating these laws in developing products, delivering services, or the conduct of their business."
- When determining who in the organization should access systems, programs, databases, or other intermediaries to security-sensitive information, management should consider policies that limit access to the minimum number of people and minimum extent necessary for employees to perform their job. Granting privileges that exceed the minimum required for proper job performance can add risk to the security and privacy of sensitive information.
- "Companies may also face information security liability for alleged privacy violations or by failing to supervise their employees. If companies roll out products or services that allegedly violate consumer privacy by accessing their applications or devices without permission, they may be sued for violating cybercrime laws."
- "In addition, if rouge employees within companies gain unauthorized access to competitors' computer systems to uncover business intelligence, they may face cybercrime claims based on the unauthorized access."

Employee Training and Management

- The cost of compliance is related to employee training and management. A financial institution's risk assessment should:
  - Check employee references and perform background checks;
  - Require employees to sign a confidentiality agreement;
  - Limit employee access to sensitive customer information;
  - Use password-activated screen savers to lock employee computers;
  - Encrypt customer files on laptops and other computers in case of theft;
  - Impose disciplinary measures for security policy violations;
  - Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names.
- The FTC noted in one of its publications that "the success of your information security plan depends largely upon the employees who implement it."
- http://knol.google.com/k/rob-scott/complying-with-the-glba-safeguards-rule/1llgytainraw9/1#

GM's Solution for its dealers

- DEALERS NEED TO: Adopt a Multi-Layer Security Strategy:

  Layer 1 - A dedicated, private Internet connection. A dedicated Internet connection like a T1 service will reduce the amount of unwanted attacks by about half.
- **Layer 2 - Securing the LAN with a reliable firewall capable of handling today's "Blended Threats"** A firewall that analyses data in real-time and monitors all traffic coming in and out of the dealership's Internet connection will help in protecting sensitive data. Intrusion methods change with technology. Dealership firewalls must be able to identify the traffic going through the firewall and be able to determine if this data is wanted, safe, and secure enough to deliver to the end user. Moreover, a managed firewall with timely updates will keep the dealership up-to-date with the newest technologies and threats.
- **Layer 3 - Securing the LAN through a repeating process of monitoring and adjusting** A security program is only as good as the party that monitors the attacks and adjusts the security policy appropriately. Without this continual process of monitoring and adjusting, a dealership will become further and further behind putting themselves at a high risk.
- **Layer 4 - Securing PCs with reliable anti-virus/spy ware protection.** Security starts from within the dealership. Since a network will be compromised at its weakest link. each PC must have up-to-date anti-virus protection. A corporate anti-virus solution is the best fit for dealerships of all sizes. Many of today's current corporate anti-virus solutions also include spy ware protection and key logger protection.
- **Layer 5 - Employee monitoring and education** Many theft occurrences start from the inside out. Usually this can be prevented by properly educating employees on ways in which they can help to protect the companies privacy and their customer's privacy. Examples include social engineering, proper passwords and storage of passwords, remembering to logout or lock their workstation when they leave, etc…
- While no dealership can be "completely" safe, securing each layer of the dealership is the best way to reduce their risk against threats from within and outside the dealership and mitigate any liability acts committed by attackers. Turning to experts in security, technology, and dealership infrastructure is the best way to make sure the dealership is better protected.

Health Insurance Portability and Accountability Act

- The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)
- It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.
- A covered entity may disclose PHI to facilitate treatment, payment, or health care operations, or if the covered entity has obtained authorization from the individual.
- Covered entities must disclose PHI to the individual within 30 days upon request. They also must disclose PHI when required to do so by law, such as reporting suspected child abuse to state child welfare agencies.
- PHI disclosures should be made with reasonable effort to disclose only the minimum necessary information required to achieve its purpose.
- The Privacy Rule gives individuals the right to request that a covered entity correct any inaccurate PHI. It also requires covered entities to take reasonable steps to ensure the confidentiality of communications with individuals.
- For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.

HITECH ACT Modifications to HIPAA

- The American Recovery and Reinvestment Act (ARRA, or The Obama Stimulus Bill), signed into law in February 2009, includes new, more comprehensive provisions for HIPAA. These provisions are in a section of the bill known as the Health Information Technology for Economic and Clinical Health Act (HITECH).
- **Changes required for Covered Entities under HITECH Act:**
- Mandatory yearly audits by Health and Human Services to make sure that you are meeting the HIPAA requirements
- Explicit fines of up to $1.5 million dollars/year for disclosures of protected health information that violate the HIPAA Privacy Rules
- Associate equally liable to damages and unfavorable publicity.
- Business Associate Agreements with vendors and partners who have contact with your organization's protected health information is now mandatory.
- New mandatory reporting requirements on unauthorized disclosures of protected health information — to those whose information was disclosed, to Health and Human Services, and for large enough disclosures, to the media.
- **For HIPAA Business Associates, HITECH imposes even more serious changes:**
- Business Associates are now responsible for following all HIPAA Privacy and Security regulations with respect to all protected health information that they obtain or generate.
- Unauthorized use or disclosure by Business Associates of any protected health information leaves the Business

HIPAA & HITECH Privacy

- The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access.
- The rights of an individual to access and control PHI pertaining to that individual have expanded under HITECH.
  - For example, an individual can prohibit healthcare providers from disclosing PHI to the individual's health plan if the individual pays for the healthcare treatment or services out-of-pocket in full.
  - Under certain circumstances, an individual may request an accounting of disclosures of PHI by a covered entity for treatment, payment, and healthcare operations when the covered entity uses or maintains an electronic health record with respect to that PHI.
  - An individual may request a copy of his or her record in electronic format or may direct the covered entity to send a copy to another entity or person. The covered entity may charge for labor costs associated with responding to the request.
  - HITECH generally prohibits covered entities and business associates from directly or indirectly receiving remuneration for any PHI of an individual without the individual's prior authorization.

Security Rule Goals and Objectives

- Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.
- As required by the "Security standards: General rules"4 section of the HIPAA Security Rule, each covered entity must:
  - Ensure the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits;
  - Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and
  - Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.
- In complying with this section of the Security Rule, covered entities must be aware of the definitions provided for confidentiality, integrity, and availability as given by § 164.304:
- Confidentiality is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity is "the property that data or information have not been altered or destroyed in an unauthorized manner."
- Availability is "the property that data or information is accessible and useable upon demand by an authorized person."

Security includes Administrative, physical and technical safeguards

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized.
- Documented risk analysis and risk management programs are required.
- Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
- Access to equipment containing health information should be carefully controlled and limited to properly authorized individuals. Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Administrative policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
- Procedures should clearly identify employees or classes of employees who will have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those employees who have a need for it to complete their job function.

HIPAA Security Rule

- The HIPAA Security Rule specifically focuses on the safeguarding of EPHI. All HIPAA covered entities, which includes some federal agencies, must comply with the Security Rule. The Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following covered entities:
- Covered Healthcare Providers— Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- Health Plans— Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- Healthcare Clearinghouses— A public or private entity that processes another entity's healthcare transactions from a standard format to a nonstandard format, or vice versa.
- Medicare Prescription Drug Card Sponsors – A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act.

Types of Safeguards

- **Security standards: General Rules** - includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.
- **Administrative Safeguards** - are defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Physical Safeguards** - are defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- **Technical Safeguards** - are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Administrative Safeguards

(a) A covered entity must, in accordance with §164.306: (1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

(C) *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3)(i) *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

Types of Safeguards

- Organizational Requirements - includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.
- Policies and Procedures and Documentation Requirements - requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.
- Standards and Implementation Specifications - each HIPAA Security Rule standard is required. A covered entity is required to comply with all standards of the Security Rule with respect to all EPHI.
  - Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard.
  - A required implementation specification is similar to a standard, in that a covered entity must comply with it.
  - For addressable implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment.

Business Associates

- Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected?

- Are there any new organizations or vendors that now provide a service or function on behalf of the organization?
- Such services may include the following:
  - o Claims processing or billing
  - o Data analysis
  - o Utilization review
  - o Quality assurance
  - o Benefit management
  - o Practice management
  - o Re-pricing
  - o Hardware maintenance
  - o All other HIPAA-regulated functions

- Have outsourced functions involving the use of EPHI been considered, such as the following:
  - o Actuarial services
  - o Data aggregation
  - o Administrative services
  - o Accreditation
  - o Financial services
- Does the agreement or arrangement specify how information is to be transmitted to and from the business associate?
- Have security controls been specified for the business associate?

Mandatory breach notification for violations

- **Mandatory notification of privacy and security breaches**
- If PHI privacy or security breaches occur, you must report them to all affected individuals and to the Department of Health and Human Services (HHS).
- If the breach affects 500 or more individuals in one state, you must also report it immediately
  - to HHS and
  - to the media.
  - Breaches affecting less than 500 individuals can be reported annually.
- Your business associates are required to report breaches to you, the covered entity.
- HHS is required to publish reported breaches on its website when more than 500 individuals are affected, including each covered entity involved in the breach.
- What is considered a security breach?
  - A security breach is defined as any use or disclosure that "compromises the security or privacy" of protected health information.
  - In addition, the breach must pose a significant risk of financial, reputational, or other harm to the individual to trigger the obligation to provide notice.

Confidential information could be at practical as well as legal risk

Some confidential data needs real protection, not just protection from legal claims of disclosure

- Industrial and national espionage, patentable inventions, valuable trade secrets, criminal investigations
  - Stuxnet virus demonstrates insecurity in most secure environments
  - Flame may have been its earlier and more general cousin
  - US government claims **Huawei** and **ZTE** pose a risk to national security
- Companies must assess the value of the information and the cost to the company of a loss to plan appropriately

Credit card data is regulated by vendors

- The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection
  - Compliance with the PCI Data Security Standard (PCI DSS) is vital for all merchants who accept credit cards, online or offline
  - PCI is theoretically voluntary, but the merchant's agreement with its bank may (and should) call for compliance
- Merchants must follow 12 requirements in the standard, as enforced by the merchant's bank
  - PCI Council claims no credit card information has been lost from a merchant which has remained in compliance – greatest lapse is failing to update and maintain
  - "If operation of your e-commerce shopping cart is outsourced to a service provider, ask it to give you annual evidence of the service's compliance with the PCI Data Security Standard."

PCI Security Standards Council Founders

PCI compliance requirements

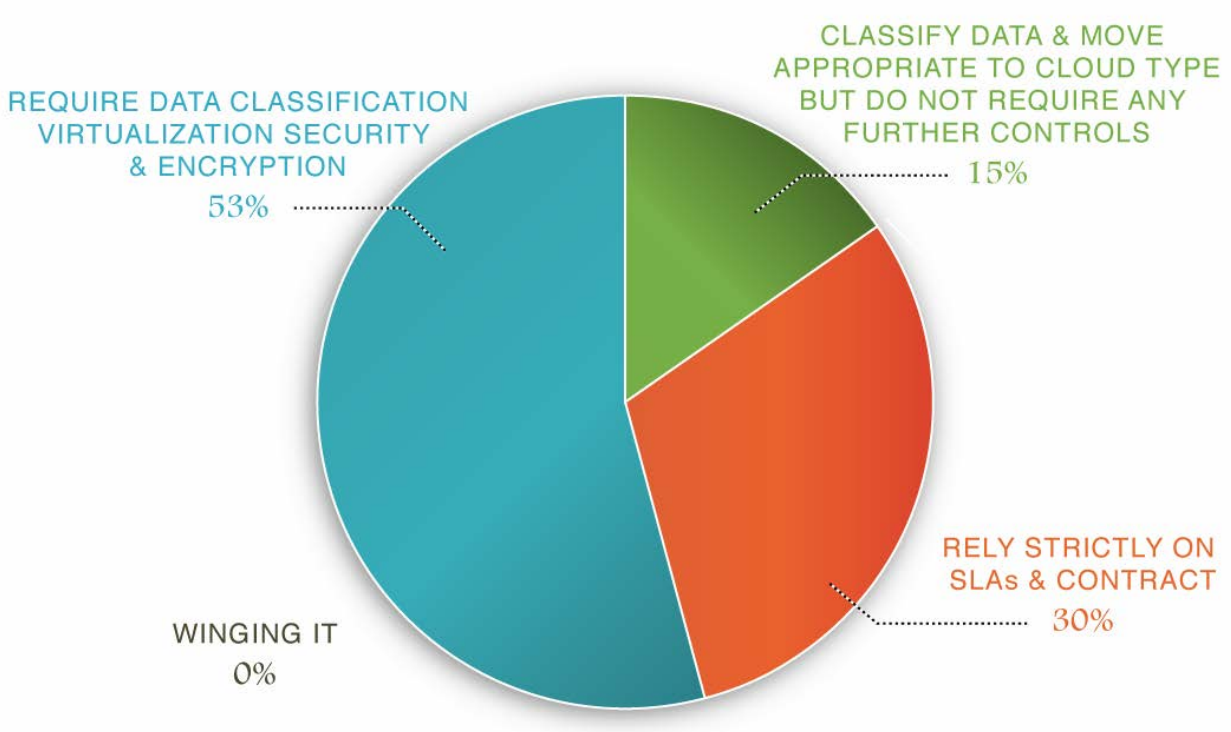
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data
	4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to 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

Before evaluating any vendor

- Conduct a comprehensive integrity, security and privacy audit
  - Understand the internal deficiencies (and that these are deficiencies)
  - Distinguish precisely which services will move to a cloud vendor and which will remain located on site
  - Distinguish the types of sensitive information and make the RFP for the cloud computing responsive to the services needed
- Assign, Identify, and Assess
  - Assign the work-flow to specific people/departments with clear lines of responsibility
  - Identify the tasks, the information, the services, and the team so everyone involved has access to the same plan
  - Assess so that a plan to move public, unregulated data does not become unduly expensive by making it GLBA compliant or that a cheap plan for simple data is used to collaborate on new patents, the disclosure of which could lose the company millions in cash and dominance in its industry

Approach to the cloud service agreement

- **Contracting approach: Trust but verify**
- Contractual duties are required but insufficient; reliance on the SLA and contract is a violation of HIPAA and likely violation of GLBA, PCI
- Companies need to evaluate much more carefully before even beginning to negotiate with a particular vendor



Before evaluating a particular vendor

- **Operational issues**
  - Is this cloud service a true core business of the provider?
  - How financially stable is the provider?
  - What is its level of technical expertise within its operations team?
  - How long has the company been offering the service, and does it have a track record with verifiable customers?
- **Legal and compliance issues:**
  - Is the company outsourcing any aspect of the service to a third party, and if so, does the third party have the appropriate arrangements with the provider?
  - Does the physical security of its datacenters meet your legal, regulatory and business needs?
  - Are its business continuity and disaster recovery plans consistent with your business needs?
  - Does the provider offer any indemnification?

Source: **Vic (J.R.) Winkler,** *Securing the Cloud: Cloud Computer Security Techniques and Tactics (Syngress 2011)*

Approach to the cloud service agreement

- **Start at the bottom (boiler plate) of the agreement**
- **Warranty**: Never enter into an agreement regarding protected data with an "as is" warranty
  - None of the assurances, duties or promises can be met with contract credits
- **Indemnification**: To what extent will the vendor pay to step into the shoes of the customer to address costs of data breach notification; loss of data resulting in fines (which can run into the $ millions); or other harms caused by vendor or vendor's employees
- **Customer's Duties**: To what extent has the contract placed security obligations and data integrity obligations back on the customer, eviscerating the protections provided
- **Negotiability**: To what extent is the service agreement or service level agreement customizable and negotiable
  - Take-it-or-leave-it generally inappropriate for valuable data
  - Too much customization will drive costs and create risks that vendor won't be competent to follow specialized duties in the agreements

Vendor duties to be specified in the agreements

- To warrant that all information provided is true and accurate and will be updated to remain accurate
  - Don't allow statements in the marketing to be disclaimed in the SLA
- To meet applicable regulatory guidelines as a covered entity or third party recipient of data
- To identify the location of data services which meet compliance needs
  - e.g., no offshore storage of HIPAA or sensitive data
- To utilize best practices to assure data privacy, security and integrity
- To report any data security breach and meet applicable state and federal notification obligations
- To manage vendor personnel in a manner that restricts access to stored information from non-essential personnel, to train its personnel to meet data privacy and security practices, and to immediately cut-off access to former employees
- To provide appropriate physical safeguards

Vendor duties to be specified in the agreements

- To physically secure the information, by controlling physical access to computers, servers and equipment
- To provide meaningful indemnification provisions
- To maintain the financial ability to meet such obligations
- To restrict exploitation of aggregate data analysis and metadata analysis
  - May depend on the nature of the regulated data
  - The aggregation of services by large vendors creates opportunities to track and study the data flow
  - Even if done on an aggregate basis, however, the use of health care or customer financial data may not be authorized and should be contractually restricted
- To specify back-up, data destruction and data integrity protocols

Specific issues of which to be mindful

- USA Patriot Act – Duty to use best efforts to fight gag orders
- To notify of any government action (unless protected by gag order)
- Audit rights
  - Right to engage in customer audit
  - Obligation to provide annual audit report at specified level
- To review (or even approve) change of control of vendor
- For HIPAA data services, to sign on as a business associate
- For GLBA, to provide disaster recovery plans and procedures
- To be fully PCI Compliant
- To enable multi-site redundancy (particularly for large commercial vendors)
- Post termination duties to maintain data and provide transition support

The details: Service Level Agreement checklist

- **Full regulatory compliance**
  - Wrap in ongoing changes to state law, federal law and regulations, and applicable industry standards
  - Specify location of data; physical security
  - Must depend on the specified nature of the content, so the nature of the content must become a material term to the agreement
  - Encryption (always while data is in motion); specify points of decryption of secure data
- **Privacy & Confidential information**
  - Broader than regulated data
  - Be specific; don't call it all confidential if it isn't
- **Service documentation and certification**
  - Specify the types and timing of reports
  - SOCS2, operating procedures and supporting documentation covering contingency plans, Disaster Recovery and Pandemic Plan
  - Executive summaries of all vulnerability assessments and penetration tests actually conducted by Company and Company response plan
  - Monitoring by third party, if appropriate
- **Metrics and Service levels**
  - Uptime/downtime guarantees
  - Operational guarantees
  - Control over definition of downtime and other performance measures

The details: Service Level Agreement checklist

- **Data practices**
  - Retention and deletion laws
  - Data, software and hardware destruction protocols (so data is fully unrecoverable when erased)
- **Transparency and Breach Notification obligations**
  - Since data may be from any U.S. (or international) jurisdiction, notification must meet most exacting standard
- **Representations and warranties**
  - Be specific with regard to obligations under warranty
  - Be sure vendor includes all factual statements in all literature
  - Warranty only valuable if company has insurance or value

- **Performance Considerations**
  - **Throughput:** System response speed
  - **Reliability:** System availability
  - **Load balancing:** When elasticity kicks in
  - **Durability:** How likely to lose data
  - **Elasticity:** How much a resource can grow
  - **Linearity:** System performance as the load increases
  - **Agility:** How quickly the provider responds to load changes
  - **Automation:** Percent of requests handled without human interaction
  - **Customer service response times**

Source: IBM, developerWorks, cloud computing editors

The details: Service Level Agreement checklist

- **Property of the parties**
  - Data owned by client
  - APIs and software owned by vendor
- **Change Events**
  - Acquisition, merger, de-acquisition, bankruptcy of each party
  - Movement of data outside U.S.
  - Change to laws and regulations
- **Limitations by Vendor**
  - Third party equipment and services
  - Exclusions of every representation and warranty
  - Liability caps
- **Cross Indemnification**
- **Events of Default**
  - Expected technical responses
  - Remedies regarding inability to provide technical response
  - Failure to pay; conflict over response
- **Termination**
  - Triggers
  - Post-termination obligation before closure
  - Post-termination obligations

The details: Service Level Agreement checklist

These issues are likely company concerns rather than legal concerns

- **Data Sources**
  - Log data, Configuration data,
  - Performance data such as network traffic, data flow and CPU utilization
  - Vulnerability data across network devices and hosts and network traffic pattern data
- **Compliance Support**
  - End-to-end encryption may not be sufficient (We're blind so we're compliant may not be sufficient)
  - Doesn't provide reporting or other tools and cannot work in SaaS
- **Interoperability**
  - Increases portability and avoids lock-in
  - Risks precluding proprietary systems
- **Analytics**
  - Business should learn from the data: who is using the platform, where are the client's customers dropping out, what trends are available
  - Dashboards, network reports, etc.
- **Reporting**
  - Data Management
  - Compression, encryption, archival services
- **Scalability**
  - Architecture
  - Performance

New audit standards available

- The SAS 70 report may have created a false sense of security because it did not set minimum standards or establish best practices.
- The American Institute of CPAs (AICPA) has replaced the SAS70 with the SSAE 16, effective June 15, 2011.
- Under SSAE 16, SOC 2 and SOC 3 reports provide much more stringent audit requirements with a stronger set of controls and requirements specifically designed around data center service organizations.

- ***Security***: The system is protected against unauthorized access (both physical and logistical).
- ***Availability***: The system is available for operation and use as committed or agreed.
- ***Processing integrity***: System processing is complete, accurate, timely and authorized.
- ***Confidentiality***: Information designated as confidential is protected as committed or agreed.
- ***Privacy***: Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and AIPCA's *Generally Accepted Privacy Principles*.

New audit standards available

- Type 1 report assesses the compliance of the vendor's efforts to meet the standards that vendor selected. If the vendor selected minimal standards, then the report will only reflect that those minimum standards were or were not met.
- A Type 2 report provides the auditors' opinion as to the accuracy and completeness, the suitability of the design of controls, and the operating effectiveness of the controls throughout a declared time period, generally between six months and one year." While there is always room for interpretation and variations among auditors, the Type 2 report has considerably more assessment value than the Type 1 report.
- A variation of the Type 2 report can be disclosed as a Type 3 report, which basically strips certain internal reporting information from the Type 2 report so that the report can be made available to potential customers and the general public.

The Type 3 report includes a certification or seal of approval that can be used by the reporting company to show its compliance with the SSAE 16 standards.

Reminders for lawyers as users

- Consumer products are not **secure**
  - Google Docs, gmail, etc. give Google non-exclusive rights in the content
  - Since 1999, the ABA recognized that legal protections of unencrypted email are sufficient to permit its use, unless there is a heightened particular risk
  - **2008 NY** ethics opinion found the computer-mediated review of email did not destroy confidentiality, but it raises questions
  - Dropbox is great for non-confidential documents, but does not encrypt in transfer – so a targeted company may be vulnerable
  - The appropriate standards are flexible, based on the size of the practice, the nature of the practice and known risks
  - Once full encryption is available, is it reasonable to still use unencrypted document storage or even e-mail communications?

- Check the service level agreement
  - Google Apps for Business doesn't give away rights
  - Only Premier edition of Google Apps for Business has commercial level security