



# **A Survey of Legal Risks in Information Security 2011**



**Jon J. Banks, EJD, CISSP**

**©2011 – All Rights Reserved**

# Agenda

- ❖ Legal Disclaimer
- ❖ About the Speaker
- ❖ Highlight a Few Security and Privacy Laws
- ❖ Brief Overview of the Legal System
- ❖ Some Legal Concepts Applicable to Information Security
  - Negligence
  - Contracts
  - Strict Liability
  - Criminal Law
  - FTC Sanctions
- ❖ E-Discovery
- ❖ Why Compliance is Not Enough
- ❖ Questions

# Legal Disclaimers

- ❖ I am **NOT** a lawyer!
- ❖ The following presentation is **NOT** intended to constitute any legal consultation, legal advice, or legal services.
- ❖ This presentation is only intended to help you gain an appreciation for the legal risks your organization may face and encourage you to seek assistance from **YOUR** legal counsel.
- ❖ All legal decisions made with respect to your organization's information security programs should be made by **YOUR** organization's legal counsel.



## About the Speaker

- ❖ **Executive Juris Doctorate** in Law and Technology (with Honors) – Concord Law School
- ❖ **CISSP, Security+**
- ❖ **13 Years in IT and Information Security**
  - Public and Private Sectors
    - Network/Security Engineering
    - Security Analyst
    - Security Operations
    - Governance, Risk, and Compliance
      - PCI (2 – Level 1 Service Providers)
      - HIPAA
  - Big Four IT Advisory
- ❖ **Specialize** in building information security programs and security architectures.
- ❖ **Published and presented** on the topics of legal risks and e-discovery in information security

## Some recent *ISSA Journal* articles have been related to information security and the law.



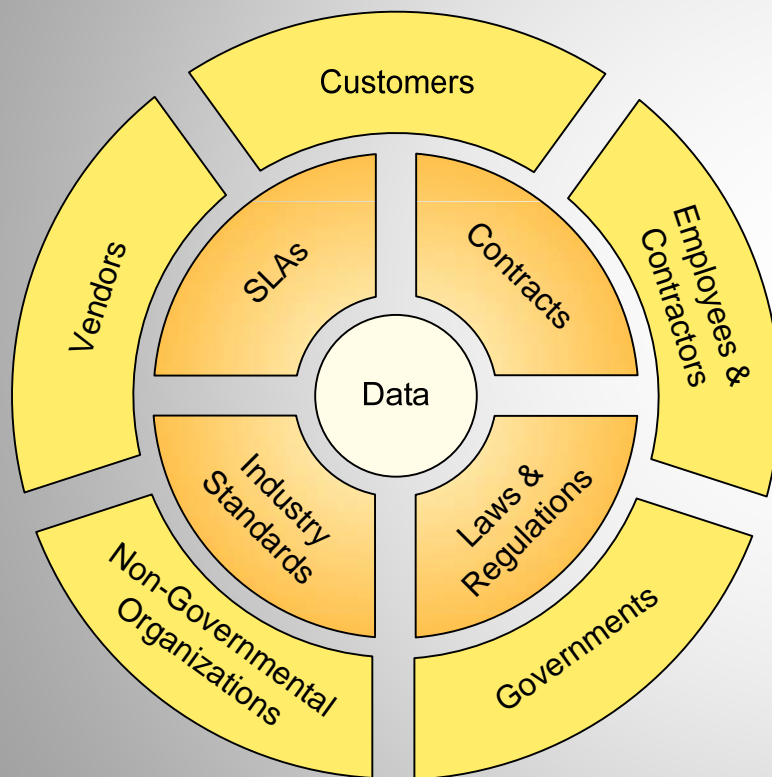
- ❖ June 2009 – *An eDiscovery Primer for Information Security*
  - Jon J. Banks
  
- ❖ January 2010 – *Information Security Breach Disclosure: When, How Much, and To Whom*
  - M. Scott Koger
  
- ❖ May 2010 – *The Legal Defensibility Era*
  - David Navetta
  
- ❖ January 2011 – *The Evolving Legal Duty to Securely Maintain Data*
  - Randy V. Sabett

We are now seeing law firms that specialize in information security and privacy.



- ❖ Established in October 2009
- ❖ <http://www.infolawgroup.com/>

## Legal risks are created as a result of relationships and interactions between your organization and other entities.



- ❖ These legal obligations are created by the organization's **relationship** and **interactions** with:
  - Customers
  - Employees, Contractors, and other Agents
  - Governments (International, Federal, State, Local)
  - Non-Governmental Organizations (e.g. PCI Council)
  - Vendors
- ❖ An organization's **legal risks** are determined by:
  - SLAs
  - Contracts
  - Laws & Regulations (Governmental)
  - Industry Standards (Non-Governmental)

## States continue to be very proactive with Information Security and Privacy legislation.

### ❖ Some State Information Security Laws

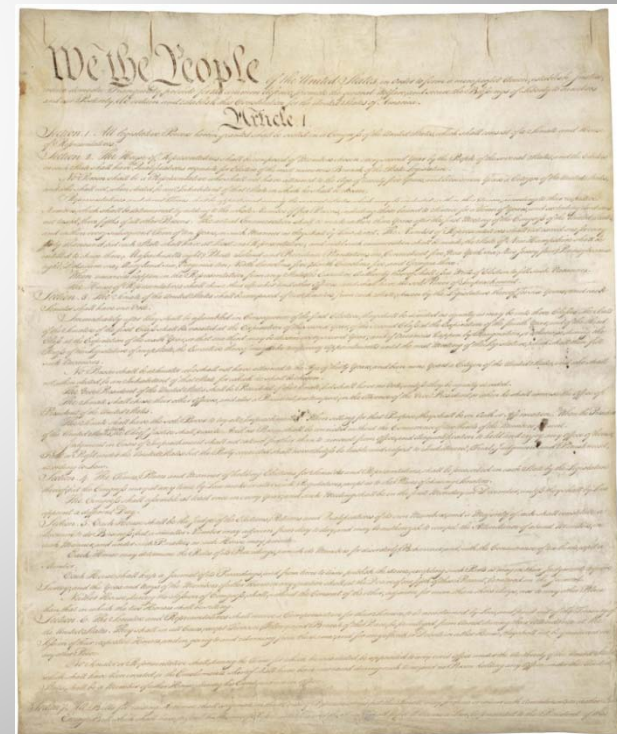
- Nevada law mandates **PCI compliance**.
  - Nev. Rev. Stat. § 603A.215
- Washington law provides for exemptions from liability if the entity is certified **compliant with PCI**.
  - Chapter 19.255.020 RCW
- Minnesota law **prohibits** retaining select card authorization data after authorization.
  - Minn. Stat. § 325E.64
- MA and NV law mandate a comprehensive **information security program**.
  - 201 CMR 17.00 et. seq.
  - Nev. Rev. Stat. § 603A.210

### ❖ Some State Privacy Laws

- CA and UT have state laws addressing the **Privacy of Personal Information**.
- CA, CT, NE, and PA have state laws addressing **Privacy Policies** on web sites.
  - <http://www.ncsl.org/default.aspx?tabid=13463>

## The majority of States have taken the issue of Security and Privacy breaches very seriously.

- ❖ All but four states have **breach notification laws**.
  - <http://www.ncsl.org/Default.aspx?TabId=13489>
- ❖ WellPoint is being sued by the Indiana Attorney General for a **delay in breach notification**.
  - [http://www.in.gov/portal/news\\_events/58723.htm](http://www.in.gov/portal/news_events/58723.htm)
- ❖ Are your Incident Response procedures up-to-date?



## The Federal Government has gotten involved in information security and privacy in certain industry verticals - Healthcare

- ❖ Federal Regulations ***mandate security standards*** for the protection of Protected Health Information (PHI) including administrative, physical, and technical safeguards and policies and procedures.
  - 45 CFR 164.302 et. seq.
- ❖ As a result of the HITECH Act of 2009 (Pub. L. 111-5), Federal Regulations related to the ***breach of PHI*** have been enacted which address breach notification including the timing, content, and method of notification.
  - 45 CFR 164.404 et. seq.
- ❖ Federal Regulations also place the ***burden of proof*** on the Covered Entity or Business Associate, as appropriate, to prove that breach notifications were made in accordance with Federal Regulations.
  - 45 CFR 164.414(b)

## The Federal Government has gotten involved in information security and privacy in certain industry verticals – Financial Institutions

- ❖ Gramm–Leach–Bliley Act (GLBA) also known as the Financial Services Modernization Act of 1999 (Pub. L. 106-102) – Financial institutions must have a policy in place to **protect personal information** from foreseeable threats in security and integrity.
  - 15 USC § 6801 et. seq.
- ❖ 12 CFR 364 Appendix B – Interagency Guidelines Establishing Information Security Standards



## Some other federal criminal laws related to information security

- ❖ **Computer Fraud and Abuse Act** – Addresses fraud and related activities in connection with a computer including unauthorized access or exceeding authorized access of a “protected computer” system.
  - 18 USC § 1030
- ❖ **Electronic Communications Privacy Act** – Addresses the protection of electronic communications in transit.
  - 18 USC § 2510 et. seq.
- ❖ **Stored Communications Act** – Addresses voluntary and compelled disclosures of stored electronic communications.
  - 18 USC §§ 2701 to 2712
- ❖ Some of these laws also provide for a ***private right to bring a civil cause of action*** (lawsuit).

## Examples of privacy and data breach laws in other countries

- ❖ **Canada** – Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Protects personal information that is collected, used, or disclosed.
    - <http://laws.justice.gc.ca/PDF/Readability/P-8.6.pdf>



- ❖ **Ireland** – Data Security Breach Code of Practice
  - Ireland's Data Protection Commissioner has a Code of Practice that addresses reporting obligations in the event of a data breach.
    - <http://www.dataprotection.ie/viewdoc.asp?DocID=1082&m=f>

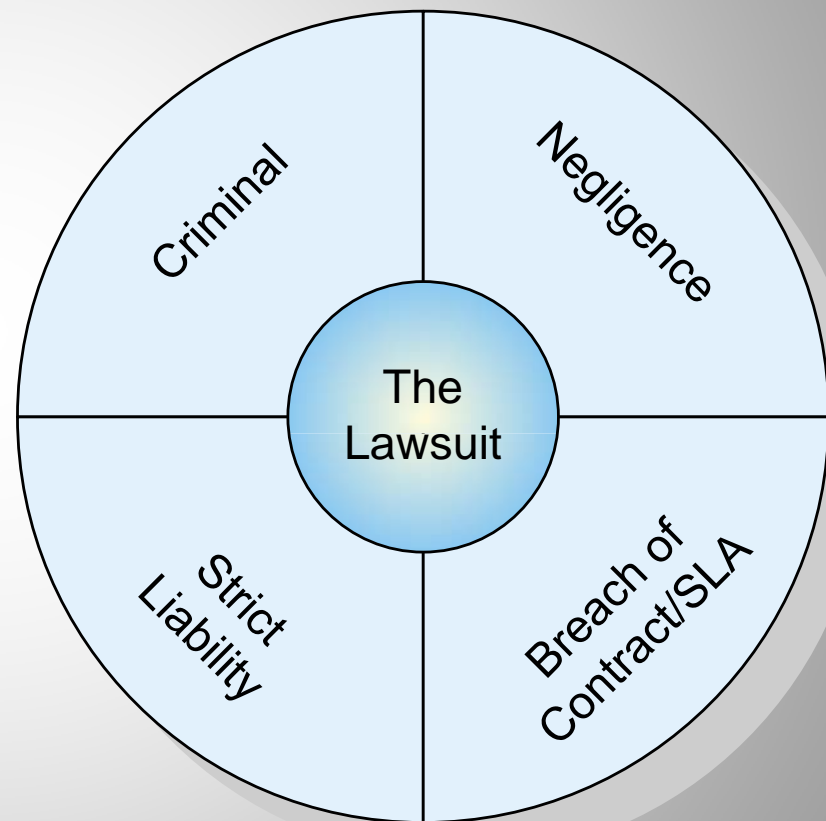
## Which court will have jurisdiction over you?

- ❖ **Jurisdiction** determines which court will hear the case, if the court can hear the case against the defendant, and which laws will apply.
  - **Laws vary** between jurisdictions.
  - Some laws are **stronger** and have greater **penalties** than others.
  
- ❖ So, how do you determine jurisdiction?
  - Where the **corporate headquarters** is located (“Nerve Center Test”)
    - The US Supreme Court held that for Diversity Jurisdiction, this test is used.
      - *Hertz v. Friend*, 130 S.Ct. 1181 (2010)
  - Where the **data centers/data** are located (“Corporate Muscle Test”), or
  - Somewhere else where it can be established were the defendant had “**minimum contacts.**”
    - *International Shoe Co. v. Washington*, 326 U.S. 310 (1945)
  
- ❖ As a result, your organization may be subject to the laws of other jurisdictions.
  - Internet
  - Think Cloud Computing

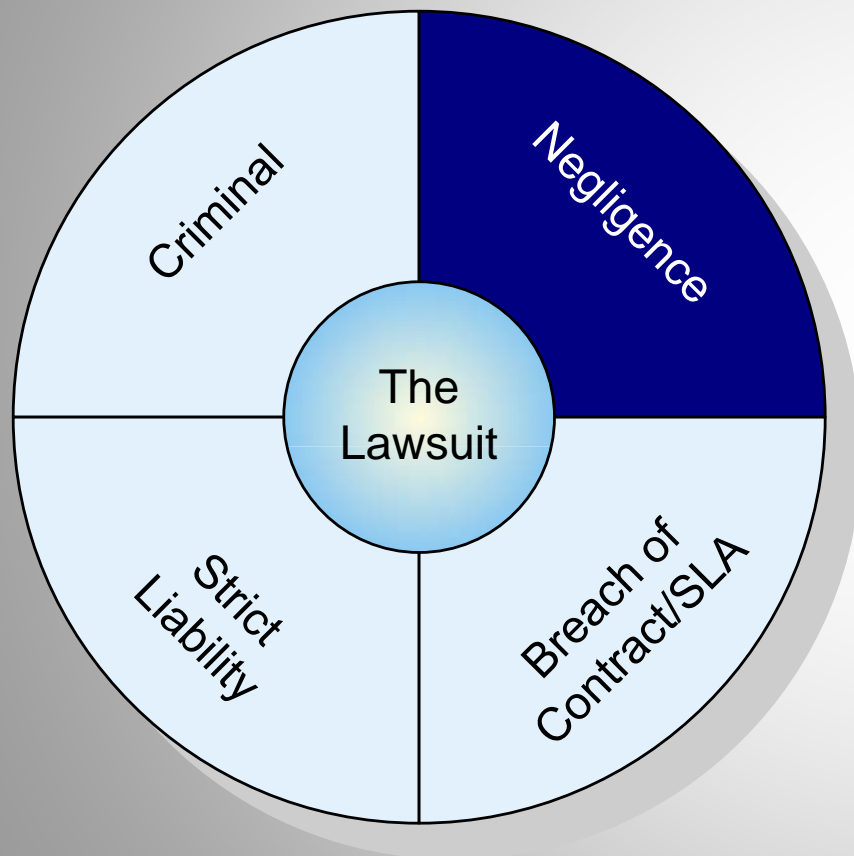


After a security or privacy breach, a lawsuit could be filed against your organization or sanctions could be imposed.

- ❖ **The Lawsuit** – After a breach, a lawsuit could be filed against your organization under one or more of the following legal doctrines:
  - **Negligence**
  - **Breach of Contract or SLA**
  - **Strict Liability**
  - **Criminal**
  
- ❖ Additionally, there could be **sanctions** brought against your organization by government agencies.



## Many civil lawsuits are based on the legal concept of Negligence.



- ❖ **Negligence** – Many civil liability lawsuits are based on negligence
  - **Duty** – To use a *standard of care* to protect confidential data
  - **Breach (of that Duty)** – Confidential data is disclosed
  - **Injury** – A customer incurs some sort of harm as a result of the unauthorized disclosure
  - **Damages** – The customer suffers some sort of damage as a result of the injury
    - Damages can be monetary or non-monetary
  
- ❖ **Standard of Care**
  - **Reasonably Prudent Person** – Most common
    - What would a Reasonably Prudent Person (or organization) do under the same or similar circumstances?
    - We are also seeing lawsuits where the standard of care is claimed to be *government or industry guidance*.

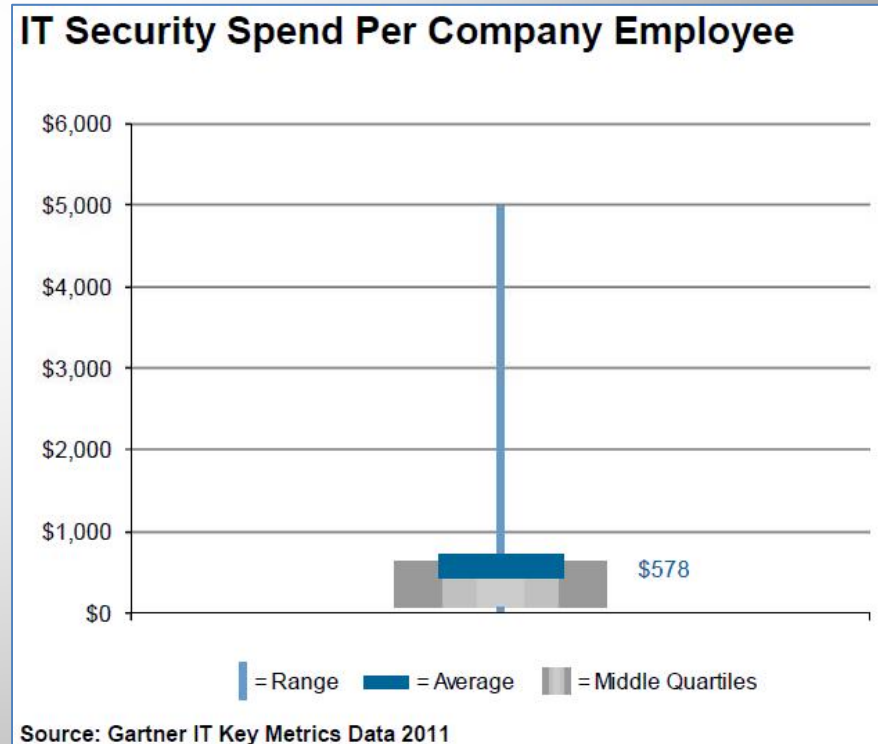
## How much should a “reasonably prudent” organization spend each year on information security?

- ❖ TXJ “Computer Intrusion”
  - Breach occurred in 2007
  - Largest breach to date based on **financial impact** to the organization.
  - To date, TJX has spend approximately \$343 million dollars in breach related expenses.
  - ***TJX continues to report activities related to this breach on its Annual Reports.***
  
- ❖ Heartland Payment Systems “Processing System Intrusion”
  - Breach occurred in 2008
  - Largest breach to date based on number of **credit cards compromised**.
  - To date, Heartland has spent \$146 million in breach related expenses.
  - ***Heartland continues to report activities related to this breach on its Annual Reports.***
  
- ❖ **Sources**
  - *TJX Annual Reports*
  - *Heartland Payment Systems Annual Reports*

# How much should a “reasonably prudent” organization spend each year on information security per employee to prevent a breach?

## THIS IS A FICTICIOUS EXAMPLE TO PROVE A POINT

- ❖ Heartland Payment Systems reported having **2,612 employees** on December 31, 2010.
  - Source: *Heartland Payment Systems 2010 Annual Report*
- ❖ Gartner reported that the **average IT security spend per employee is \$578**.
  - *Gartner IT Key Metrics Data 2011 Summary Report*
- ❖ So, if Heartland spends \$578 for each of their 2,612 employees, their total IT security spend would be **\$1,512,048.00!**
  - That's **1.03%** of the cost of the breach!
- ❖ Question: Would \$1.5 million in IT security spending be a **reasonable** amount of money to spend each year to prevent a \$146.1 million dollar breach?

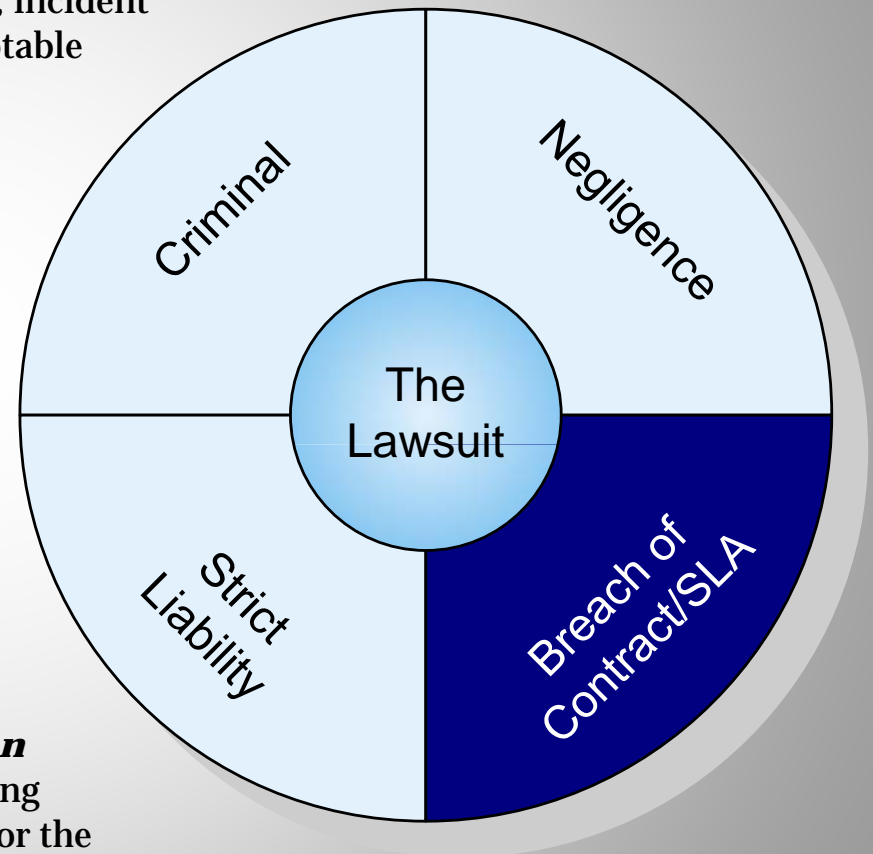


## Some examples of recent lawsuits involving negligence related to information security.

- ❖ *Shames-Yeakel et al v. Citizens Financial Bank*, 1:2007cv05387 (N.D. IL, 2007)
  - The lawsuit was brought after the customer's online bank account was breached.
  - The court would not dismiss the **negligence claim** against the bank.
    - On summary judgment, the Court stated that the bank's **failure to implement two-factor authentication** may have been a **breach of duty** to protect customers.
  
- ❖ *Cooper v. Heartland Payment Systems, Inc.*, (D. NJ, 2009)
  - The lawsuit was brought claiming Heartland was **negligent in protecting customer's information and negligent in discovering the breach**.
  
- ❖ *Choice Escrow v. BancorpSouth*, 1031-CV17436 (Cir. Court. of Greene Co., MO, 2010)
  - The lawsuit was brought after a hacker fraudulently wire transferred money out of the customer's bank account.
  - The lawsuit claimed that the security procedures and authentication methods used:
    - **Were not commercially reasonable methods** for providing security, and
    - **Were contrary to FFIEC guidance**.
  - The lawsuit also claimed that the breach constituted a **violation of the Gramm-Leach-Bliley Act**.

## Laws, regulations, and standards are now mandating contractual requirements between parties.

- ❖ **Contracts** - Due to the proliferation of laws, government regulations, and industry standards, more contracts are mandating **technical and security requirements** (e.g., encryption standards, incident response procedures, compliance requirements, acceptable use, etc.).
- ❖ As a result of the HITECH Act (Pub. L. 111-5):
  - Federal Regulations now **require** Covered Entities to have written contracts with their Business Associates that obtain or create Protected Health Information (PHI).
    - 45 CFR 164.502(e)(2)
  - Federal Regulations also **mandate certain required terms** that must be included in the contract.
    - 45 CFR 164.504(e)(1)
- ❖ PCI DSS 2.0, Requirement 12.8.2 **requires a written agreement** with your Service Providers acknowledging that the Service Provider knows they are responsible for the security of cardholder data they process.



## Cloud Computing has numerous legal considerations of its own.

- ❖ Well-negotiated contracts are even more important when using **Cloud Computing**.
- ❖ Some contract terms to consider are:
  - **Where will your applications and data be processed or stored?**
    - To what **jurisdictions** will your cloud provider unknowingly subject you?
      - Will you be in compliance with **Import/Export** Laws?
      - Will you be in compliance with **Privacy** Laws?
  - **How will you and the cloud provider handle service of process, subpoenas, and e-discovery?**
  - **Are performance expectations and responsibilities clearly addressed in Service Level Agreements (SLAs)?**
  - **How will security issues be handled and by whom?**
    - Lost/Stolen Backups
    - Unauthorized Physical Access
    - Lost/Compromised Log Files
    - Physical Theft
    - Natural Disasters

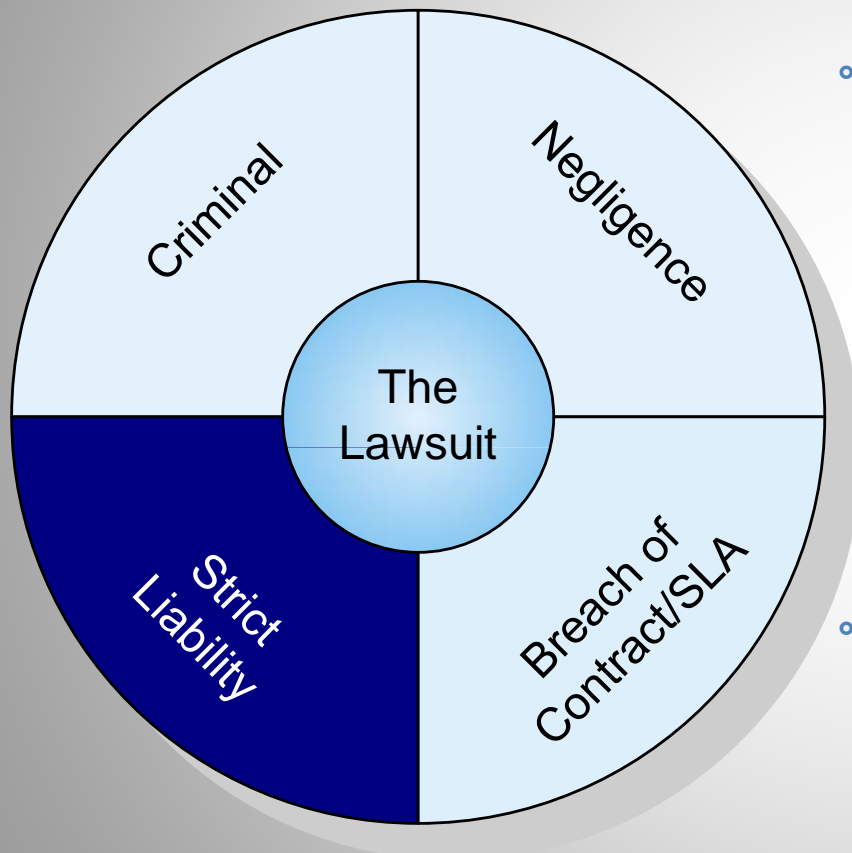
## Cloud Computing has numerous legal considerations of its own. (continued)

- **Who has which roles and responsibilities for:**
  - Data Protection?
  - Risk/Vulnerability Assessments/Pen Testing?
    - PCI
    - SAS 70/SSAE 16
    - SOX
    - HIPAA, etc.
  - Business Continuity/Disaster Recovery?
  
- **What actions will take place at the termination of the relationship or contract?**
  - Are you assured of the return or secure disposal of your data?
  
- ❖ When it comes to Cloud Computing, ***EVERYTHING*** needs to be spelled out in the contract in advance!
  
- ❖ **Resources**
  - Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing*
  - *ENISA Cloud Computing: Benefits, risks, and recommendations for information security*, November 2009

# NIST SP800-144 - Guidelines on Security and Privacy in Public Cloud Computing

- ❖ “The ***terms of service cover other important details*** such as licensing of services, criteria for acceptable use, service suspension and termination, limitations on liability, privacy policy, and modifications to the terms of service.” p. 7
- ❖ “Among the concerns to be addressed are whether the laws in the ***jurisdiction*** where the data was collected permit the flow, whether those laws continue to apply to the data post transfer, and whether the laws at the destination present additional risks or benefits.” p. 14
- ❖ “The organization’s ***ownership rights*** over the data must be firmly established in the service contract to enable a basis for trust.” p. 17
- ❖ “...service arrangements should include some means for gaining ***visibility into the security controls and processes*** employed by the cloud provider and their performance over time.” p. 18
- ❖ “The organization should ensure that ***all contractual requirements are explicitly stated in the SLA***, including privacy and security provisions. The agreement should include definitions of both the organization’s and the cloud provider’s roles and responsibilities.” p. 35
- ❖ **Source**
  - [http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144\\_cloud-computing.pdf](http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf)

## Your organization could be held liable for the actions of your employees and contractors regardless of your organization's fault?

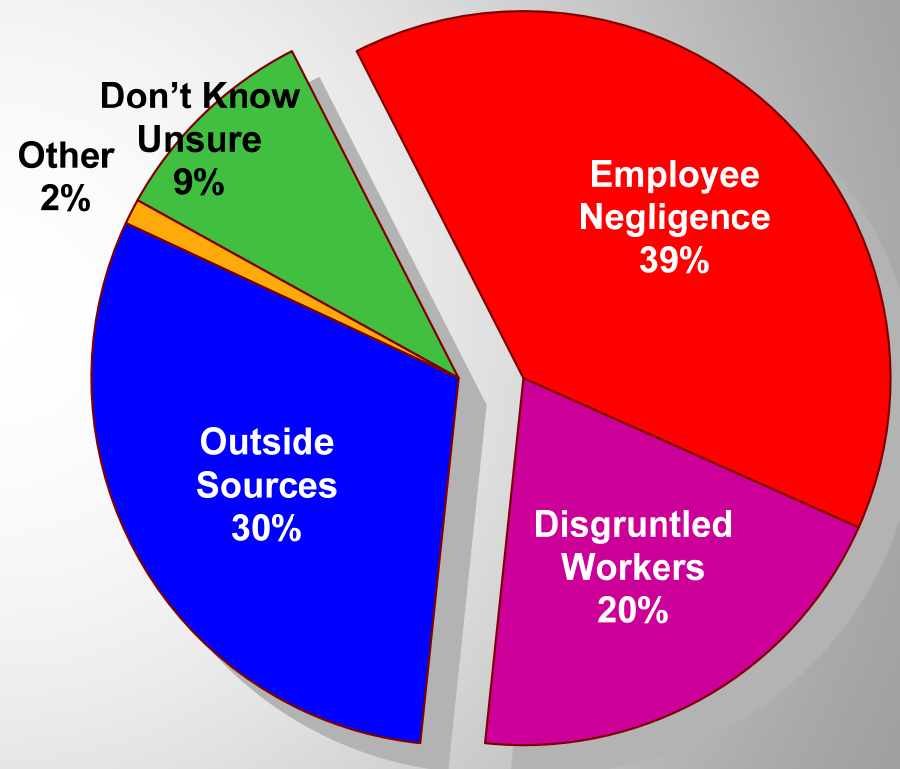


❖ **Strict Liability** - An organization is considered liable regardless of their fault or culpability.

- Under the legal doctrine of ***Vicarious Liability***, organizations could be held liable for the actions of their ***employees*** and ***contractors*** as well as other ***third parties*** acting on their behalf (agents).
  - What if an employee/contractor/agent:
    - Libels someone on a blog?
    - Steals intellectual property while at work?
    - Uses company resources to commit a criminal act?
- Do your ***policies*** address Employee/Contractor behavior and Acceptable Use?
  - Are you actively ***enforcing*** your policies?
- Do you have ***non-disclosure agreements*** in place?

## Almost 2/3 of all data leakage threats and the associated legal risks are from internal sources.

- ❖ **Internal Risks** can include both:
  - **Negligent**, yet unintentional, acts
  - **Malicious** acts
- ❖ In a 2008 Cisco study, **59%** of IT professionals surveyed cited **internal risks** as their top data leakage concern.
  - 11% admitted to **stealing** data or devices and **selling** this to third parties or knowing someone who did.
  - 9% had reported company-issued technology as either **lost** or **stolen**.
  - Concerning data leak sources:
    - 33% were concerned with **USB devices**
    - 25% were concerned with **email**
    - 11% were concerned with **stolen laptops**



Source: *Data Leakage Worldwide: The Insider Threat and the Cost of Data Loss*, August 2008

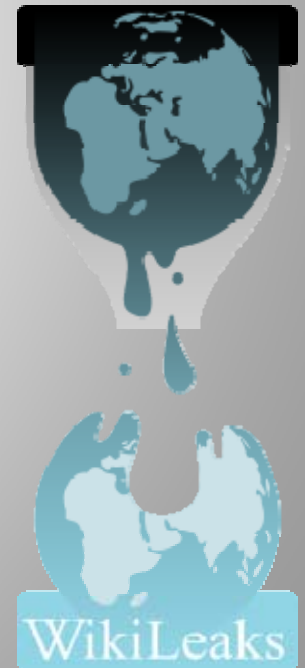
## Malicious acts from internal sources



- ❖ WikiLeaks

- ❖ PFC Bradley Manning

- This was someone **internal** that had **legitimate rights** to access sensitive information but no **need** to know.
- **No access controls** to stop him.
  - He allegedly was downloading and burning all this data to CDs.

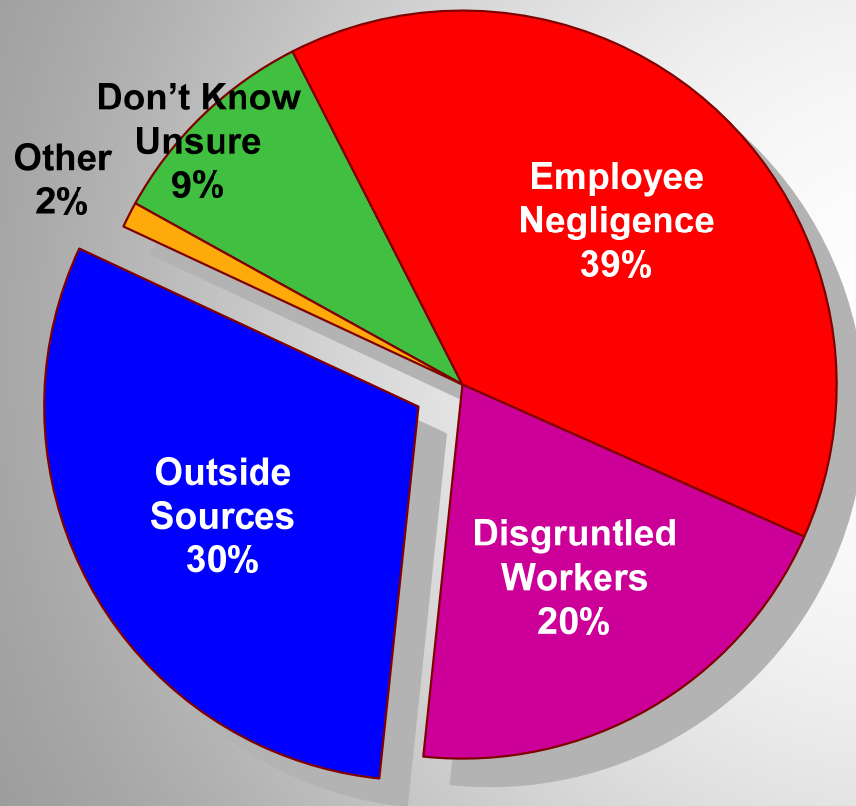


## Negligent acts from internal sources

- ❖ Are the people responsible for your organization's information security:
  - ***Qualified?***
  - ***Experienced?***
  - ***Formally Educated or Trained?***
  - ***Certified?***
  - ***Skilled?***
  
- ❖ How serious is this problem in our industry?
  - The Department of Defense addressed these issues in DoD Directive 8570 – *Information Assurance Workforce Improvement Program*
  
  - *Cybersecurity Act of 2009, § 7 (S.773):*
    - The Secretary of Commerce would have created a licensing, certification, and recertification program.
    - It would have been ***unlawful*** to provide cybersecurity services for critical infrastructure if you were not ***licensed or certified***.
  
- ❖ Would your security and privacy staffing and management be considered “reasonable”?

## In some cases, former employees and contractors could be legal risks after leaving an organization.

### ❖ What's their **motivation**?



Source: *Data Leakage Worldwide: The Insider Threat and the Cost of Data Loss*, August 2008

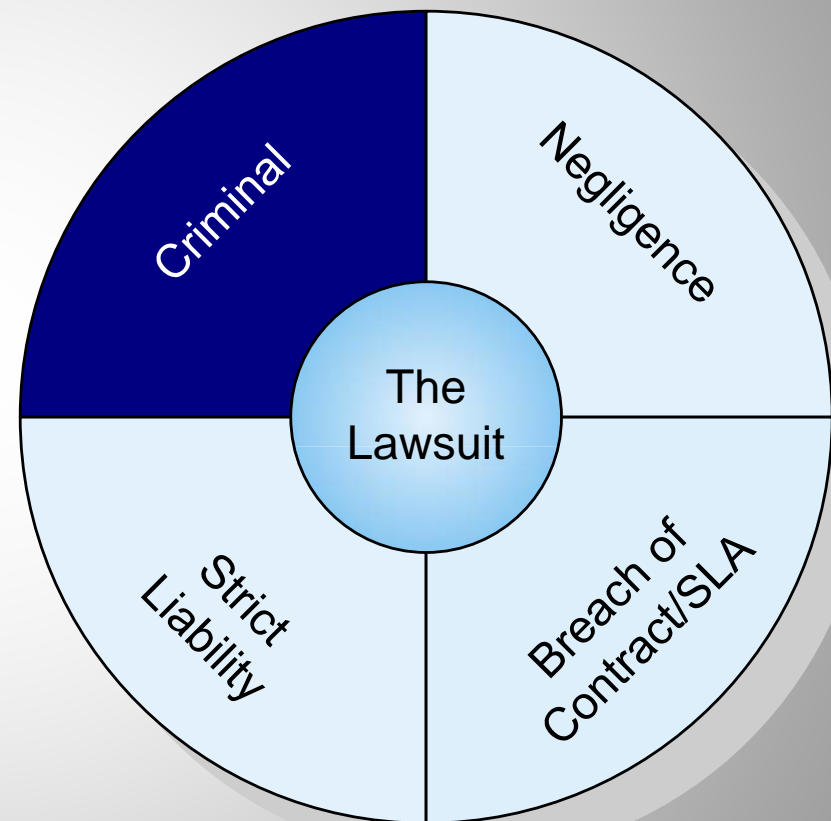
- The 2008 Computer Security Institute *Computer Crime Report* found that **financial gain is the biggest motivator for computer based crimes.**
  - A **laid-off** systems administrator was charged with blackmailing his former employer for a better severance package and excellent references. He threatened to **damage the systems** of his former employer if his demands were not met. (Source: *Computerworld*, November 13, 2008)
- And, sometimes, their motivation is just **misplaced.**
  - Terry Childs, a former San Francisco IT **employee** was found guilty of denying computer services after locking everyone out of the network—a felony. (Source: *ComputerWorld*, April 27, 2010)

## Criminal charges could be filed in the security or privacy breach if applicable laws are violated.

### ❖ **Criminal liability** against an organization or individual could be imposed:

- When an incident was the result of:
  - Gross negligence,
  - Professional misconduct, or
  - Malicious actions
- For serious violations of such laws as Sarbanes-Oxley (SOX), the Computer Fraud and Abuse Act (CFAA), etc.
- For impeding a legal investigation/procedure.
  - Refusing to produce evidence
  - Destroying evidence

- ❖ A former Goldman Sachs computer programmer was found guilty of violating the Economic Espionage Act and the Interstate Transportation of Stolen Property Act for stealing trade secrets (source code) **on his last day of employment**.
  - *U.S. v. Aleynikov*, 1:10-cr-00096, (S.D. NY 2010)



## Is your organization making material misrepresentations about your security and privacy compliance?

- ❖ **Fraud**– Can be a criminal or civil matter.
  - **Intentional Misrepresentation** – One person intends to misrepresent something to another person or organization.
  - **Material Fact** – The misrepresentation is of a fact that is material.
  - **Justifiable Reliance** – The victim does not know the misrepresentation is false and is justified in relying upon it.
  - **Damages** – As a result of this reliance, the victim suffers damages.
    - Damages can be monetary or non-monetary.
  
- ❖ Are intentional actions taking place within your organization meant to misrepresent your security or privacy compliance to another party in order to pass:
  - Internal Audit
  - SOX
  - PCI
  - FFIEC
  - HIPAA
  - Anything else

## A security or privacy breach could result in government agencies imposing sanctions or taking other actions against your organization.

- ❖ The ***Federal Trade Commission*** (FTC) can bring complaints against organizations for data breaches.
  - Breaches are considered ***Unfair Trade Practices***
- ❖ The FTC can:
  - Issue a voluntary ***consent decree***
  - File an ***administrative complaint*** with a hearing before an administrative law judge
  - File a ***Federal lawsuit***



## Some examples of FTC sanctions for security breaches and privacy violations.

- ❖ As a result of the **TJX data breach**, the FTC required TJX to:
  - ***Establish a comprehensive information security program***, and
  - Submit to data security audits every two years for the next 20 years.
  
- ❖ As a result of the **Dave & Busters credit and debit card compromise**, the FTC required Dave & Busters to:
  - ***Establish a comprehensive information security program***, and
  - Submit to data security audits every two years for the next 10 years.
  - In addition, the proposed settlement contains standard record-keeping provisions to allow the FTC to monitor compliance.
  
- ❖ As a result of **Google's failure of to follow its privacy policy**, the FTC required Google to:
  - Stop misrepresenting the company's compliance with privacy, security, and other compliance programs including the U.S.-EU Safe Harbor Framework,
  - Give Google users clear and prominent notice and to obtain express affirmative consent prior to sharing Google user's information with any third party, and
  - ***Establish a comprehensive privacy program***.
  
- ❖ **Source**
  - Federal Trade Commission (<http://www.ftc.gov>)

## What is E-Discovery?



- ❖ What is **Discovery**? If a civil (non-criminal) suit is not settled and does not get dismissed by the court:
  - Each person **shows** the other what evidence they will present in court to support their case.
    - *Generally*, you **cannot** use evidence in court if you don't disclose it during discovery.
  - Each person can also **request** from the other **identifiable** evidence which will support their case.
    - If you don't produce the evidence requested, the court **could rule against you** on the issue the evidence relates to and/or impose other punitive actions.
      - This is why e-discovery is so important and needs to be properly addressed **before** a lawsuit!

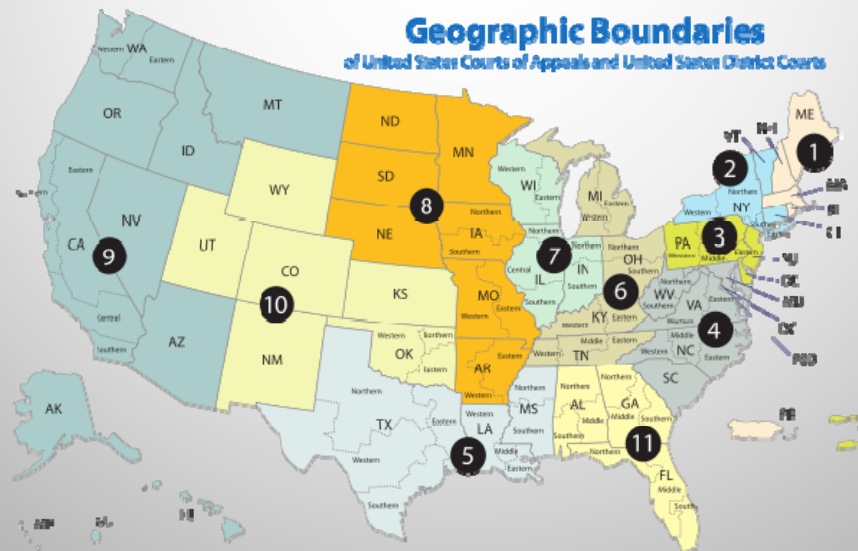
## Does your E-Discovery program enable you to quickly, easily, and inexpensively produce evidence during discovery?

- ❖ Under the *Federal Rules of Civil Procedure*, **the scope of discovery is very broad!**
  - As information security professionals, we need to know:
    - What data we have
    - Where the data is stored
    - What formats the data is stored
- ❖ Once litigation is **pending** or **anticipated**, routine operations must be **modified** or **suspended** in order to preserve electronically stored information.
- ❖ *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D. NY 2003)
  - UBS **could not produce evidence** (emails) requested during discovery and **lost the case** on the issues which related to those emails.
  - Amendment to the *Federal Rules of Civil Procedure*, December 1, 2006



## Any evidence produced during E-Discovery must be admissible in court.

- ❖ Some evidence may not be admissible in court unless it is created and maintained in the course of a **regularly conducted business process**.
  - **Unmonitored log files** may be considered hearsay evidence and would be **inadmissible**.
- ❖ To authenticate electronically stored information, a **qualified witness** may need to testify about the record and the process that created it.
  - Make sure your processes are **documented** accurately and **kept up-to-date**.
  - Determine persons **best qualified** to testify.
- ❖ *In Re Vee Vinhnee*, 336 B.R. 437 (9th Cir. BAP, 2005)



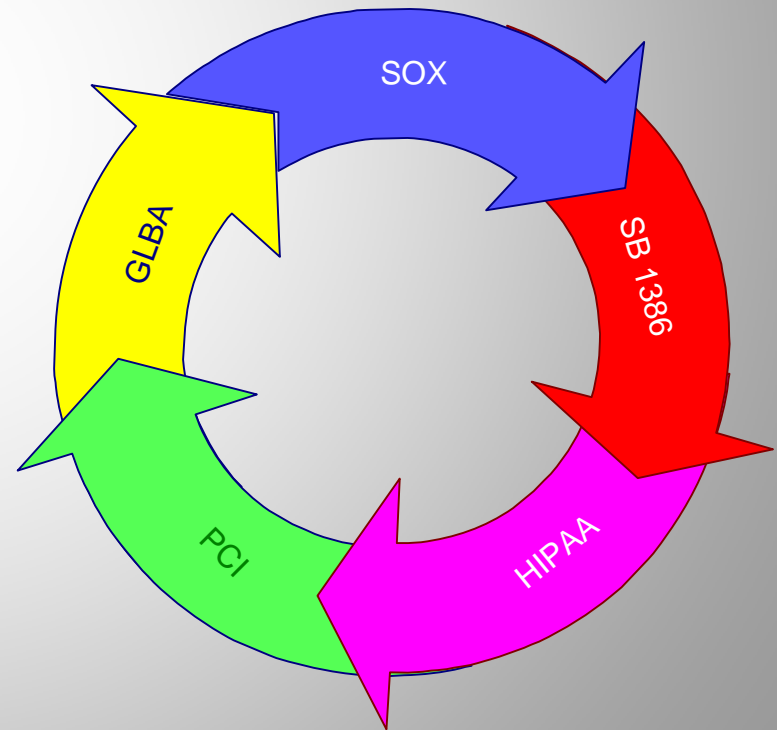
## Recent security breaches have proven numerous times that compliance is not enough!



- ❖ **Hannaford Brothers (February 2008)**
  - Estimated that 4.2 million cardholders affected.
  - Certified as ***PCI Compliant*** at the time of breach!
  
- ❖ **RBS WorldPay (November 2008)**
  - Estimated that 1.5 million cardholders affected.
  - Certified as ***PCI Compliant*** at the time of breach!
  
- ❖ **Heartland Payment Systems (January 2009)**
  - Estimated over 130 million cardholders affected.
  - Certified as ***PCI Compliant*** at the time of breach!
  - ***Seven days*** after making the announcement, a class action lawsuit was filed against Heartland.
    - *Cooper v. Heartland Payment Systems, Inc.*, (D. NJ, 2009)
    - ***18 more lawsuits*** were filed over 6 months

## Don't let your compliance with a regulation or standard give you a false sense of "security"?

- ❖ Many organizations make the **mistake** of assuming that if they are "**compliant**" with security or privacy standards or regulations, then their organization is **completely** safe.
- ❖ Why must you do **more** than comply with a standard or regulation?
  - **Standards** are created by a consensus of various industry stakeholders.
  - **Regulations** are created by a governmental entity in response to a problem.
  - Each is created for a very **specific purpose**.
    - **PCI** for Credit Cards
    - **FFIEC** for Financial Institutions
    - **HIPAA** for Protected Health Information
    - **SOX** for Financial Reporting Integrity
    - Etc.



## Don't let your compliance with a regulation or standard give you a false sense of "security"?



- ❖ Standards and regulations **never** represent the maximum effort that can be taken to address security or privacy in most organizations.
- ❖ In other industries, compliance with a government regulation or industry standard was a **minimum** requirement and did not relieve organizations from doing **more**.
  - Pharmaceutical Industry – FDA Approval
  - Aviation – FAA Certification
- ❖ **Are you auditing your way to insecurity?**
  - Are you building a comprehensive and effective information security program or merely a “compliant” one?
    - “No inspection-ready unit every survived combat.”
      - Are you preparing for **inspection** or **combat**?

## Is your organization doing more?

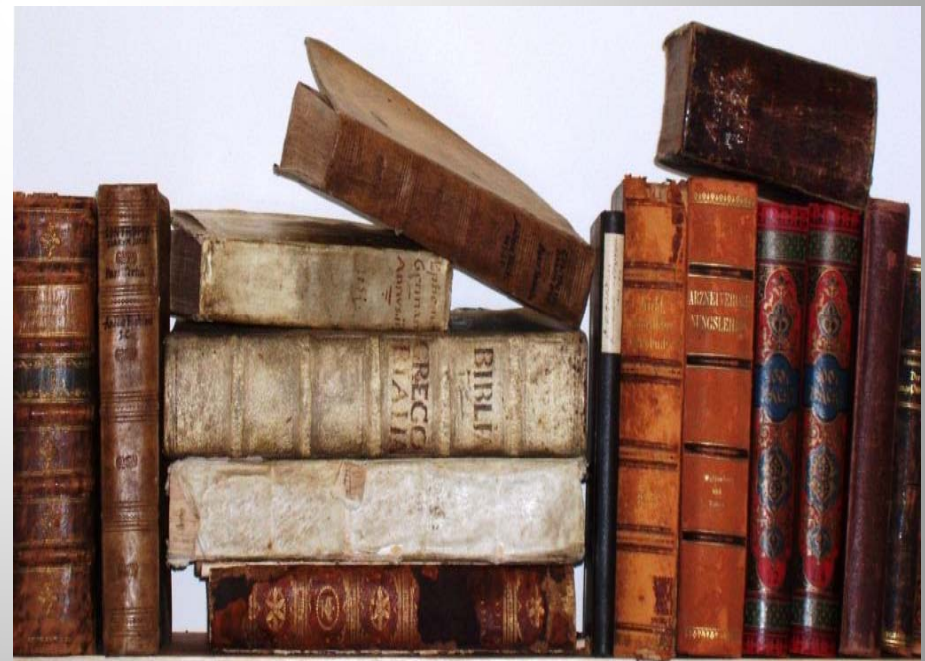
❖ “Heartland executives were well aware before the Data Breach occurred that the ***bare minimum PCI-DSS standards were insufficient*** to protect it from an attack by sophisticated hackers. For example, on a November 4, 2008 Earnings Call with analysts, Carr remarked that ‘[w]e also recognize the need to move beyond the ***lowest common denominator of data security, currently the PCI-DSS standards***. We believe it is imperative to move to a higher standard for processing secure transactions, one which we have the ability to implement without waiting for the payments infrastructure to change.’ Carr’s comment confirms that the ***PCI standards are minimal, and that the actual industry standard for security is much higher.***”

- *In Re: Heartland Payment Systems, Inc. Customer Data Security Breach*, 4:09-md-02046 (S.D. TX, 2009) paragraph 56.
- (Mr. Robert Carr is Heartland’s Chairman and CEO)

Q. “Isn’t my General Counsel addressing this?”

A. “Probably not!”

- ❖ General Counsel usually specializes in **contract** and **employment law** and not information security or privacy.
- ❖ It’s a very **young, immature** field of law with few legal “**experts**,” and there are few **leading cases** on information security and privacy although this is starting to improve.
- ❖ Nevertheless, **YOU** need to get your General Counsel **actively engaged**.
  - They are still in the best position to understand the legal risks as they relate to **your** organization.
- ❖ People possessing **legal, technical, and business** skills are needed to bridge the communication gaps between General Counsel, IT security professionals, and senior business leaders.



## Final thought: “When will organizations start taking legal risks seriously?”

1

- When we start having major breaches that are headline news.

2

- When our laws catch up and become more technically sophisticated.

3

- When younger, technology savvy lawyers and judges become more pervasive in the legal system.

4

- When lawyers realize how easy it is to get **multi-billion** dollar judgments against organizations and stop settling out of court.

- ❖ Could you find 12 **impartial** jurors today that:
  - haven't been the victim of identity theft or a security or privacy breach,
  - known someone that has, or
  - live in fear of this happening to them?

## Questions?

- ❖ Answer #1 – *“It depends.”*
- ❖ Answer #2 – *“Ask your General Counsel.”*
- ❖ Answer #3 – *“Yes, you can have a copy of the presentation.”*

# Questions?



Jon J. Banks, EJD, CISSP

pilot@ILoveToFly.org

 <http://www.linkedin.com/in/jonjbanks>

