The greatest risk, however, is loss of reputation. With healthcare organizations competing for business, it is crucial that consumers are able to trust their provider. Part of that trust has to do with how their information is used and secured.

Introduction
Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. This is a concept that has long been wrestled with at many levels of business and government. Unfortunately, it is a hard concept to grasp...until it grasps you. It's all too human to dismiss risk as an amorphous and intangible possibility, rather than a very real probability if ignored. This is the crossroad that we find ourselves at with HITECH and healthcare privacy and security today.

Executive Summary
It has been 14 years since the enactment of The Health Information Portability and Accountability Act (HIPAA)—the Privacy and Security provisions have now been in effect for 7 and 5 years, respectively; however, it is only recently that we are beginning to understand the impact and intent of what has become a wave of regulatory focus on the protection of privacy and security, especially as it pertains to an individual's health information.

As indicated in the Centers for Medicare and Medicaid (CMS) HIPAA Compliance Review Analysis and Summary of Results (2008 and 2009), there has been a fundamental lack of focus on risk assessments by most covered entities. Specifically, according to CMS analysis, many covered entities fell into one of the following categories: a) Have not performed a risk assessment; b) Did not have a formalized, documented risk assessment process; c) Risk assessment is outdated; or d) Assessment did not address all potential areas of risk.

With the latest installment of Privacy and Security mandates brought about by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the healthcare industry is finding that, yes, HIPAA is here to stay. Not only that, but now Covered Entities and Business Associates need to 'prove' that they're actually doing what their policies and procedures state and that there are controls to ensure the credibility of their compliance (HIPAA/HITECH) program.

Why Conduct a Risk Assessment
If one asks themselves why conduct a HITECH Risk Assessment, today, the answers are surely more poignant than 5 or more years ago. Whether it is the increased fines of up to $1.5 million, or the fact that the State Attorney General can bring a civil action to your doorstep, or that the Office for Civil Rights (OCR) is now mandated to conduct audits, there is certainly a greater air of seriousness and more teeth behind the legislation.

Furthermore, according to a recent study by the Identity Theft Resource Center, data breaches in the healthcare sector are occurring at a higher rate than in other industries. The study found that of the 385 data breaches that occurred in the U.S. in the first half of 2010, 30% of those affected were healthcare providers. With the dawn of Electronic Healthcare Records and the mandate to go to this system by 2014, there is an abundance of personal health information that could be at risk. With the additional notification requirements that could potentially shed a negative light on the business, healthcare organizations and any covered entities should take preemptive measures to address potential data breach risks.

The greatest risk, however, is loss of reputation. With healthcare organizations competing for business, it is crucial that consumers are able to trust their provider. Part of that trust has to do with how their information is used and secured.

Rather than continue to wrestle with unruly risks, which may or may not be known, one only needs to conduct a basic, yet comprehensive, risk assessment and know for sure where the
Risk Assessment in a HITECH World

demons of risk are. And, more importantly, know what to do when you find them.

Conducting a HITECH Risk Assessment
The risk assessment process varies according to an organization’s particular business needs and available skills. However, at its core, the most basic risk assessment process must answer the questions: What is at risk? What can go wrong? What is the probability that it would go wrong? What are the consequences if it does go wrong?

Risk assessment processes require the definition and inventory of systems and the business processes they support; an assessment of potential vulnerability and threat; a decision to act or not; evaluation of the effectiveness of the action; and communication about decisions made. Once these steps are completed, the process should be repeated on a regular basis to ensure that the decisions made and controls implemented remain effective in reducing risk and meeting business needs and goals.

Risk Assessment Phases:
Phase I: Inventory of Systems and Processes
- Identify the technologies, processes and people that interact with personal health information (PHI)
- Align assessment with organization’s business objectives and/or mission

Phase II: Threat and Vulnerability Assessment
- Methodically consider accidental breaches, destruction or alteration of data, and unauthorized disclosures
- Determine likelihood of risk occurrence
- Identify possible accidental vs. intentional vulnerabilities/exploits
- Identify possible internal vs. external vulnerabilities/exploits
- Identify reasonably anticipated harm
- Define risk ranking (likelihood and cost of each identified vulnerability/exploit)

Phase III: Evaluation of Controls
- A perfect control reduces a threat/vulnerability to zero
- Establish a control that reduces (or eliminates) the risk for each actionable vulnerability/exploit (from Phase II)
- Each control should be measurable in terms of effectiveness

Phase IV: Decision
- Decide how to manage the identified and ranked risks
  - Accept the risk (do nothing)
  - Mitigate the risk (implement identified controls)
  - Transfer the risk (e.g., buy insurance)

Phase V: Communication and Monitoring
- Ongoing communication and regular monitoring are the best ways to ensure ongoing program success
  - Develop policies and procedures that match what you do (avoid saying one thing, but doing it differently)
  - Find ways to communicate regularly to business-process owners about risk and what it means to them
- Create an annual risk assessment program calendar that allows for monitoring and review of action plans; policies and procedures; and contemplation of the program’s ability to reduce risk
- On an annual basis, adjust the risk program to reflect any new risks that need to be addressed, or past risks that can be retired

The Incident Preparedness Plan
With the risks as high as they are in some cases, it is vital that healthcare organizations conduct Incident Preparedness Planning in conjunction with the Risk Assessment Plan. This plan should be re-evaluated on an annual basis. Here are some key considerations for what should be included in your organization’s Incident Preparedness Plan:

- Create an Incident Response Team
  - Include a team of individuals from various parts of the organization who will be responsible for rolling out the plan should a data breach occur
  - The team could also help prepare the organization by conducting training for protocol for data breach response
- Conduct Breach Preparedness Training
  - Communicate what employees can do to secure data more effectively
  - Help the organization develop policies that reinforce the securing of PHI
  - Communicate policies to covered entities
- Invest in Infrastructure & Update Policies
  - When possible invest in the proper security software, encryption devices, and firewall protection to at the very least meet minimum standards
  - Ensure that the proper policies are in place when using different devices to access data
- Engage an experienced Data Breach Service Provider that will be prepared to handle the following when a data breach occurs:
  - Handle notification of the breach
  - Conduct Fraud Resolution
  - Provide Call Center Support
  - Provide Reporting
  - Provide Credit Monitoring/Identity Protection Products and Solutions that include things such as Internet Scan and Lost Wallet solutions that help consumers report, cancel and reissue items such as, credit, debit and medical and dental insurance cards

To learn more about data breach resolution, visit www.Experian.com/DataBreach, or contact Experian® at DataBreachInfo@Experian.com or 1 866 751 1323.

For more information about revenue cycle services or HITECH risk assessments, visit www.sinaiko.com.