February 1-3, 2012

Miami Beach Convention Center • Miami, Florida

MSPAlliance

MSPWORLD™

The Fusion of Cloud & Managed Services

Your chance to gather with the best and brightest minds in the managed services industry.
Engage in thought-provoking debates on major issues.

www.mspnews.com/MSPworld/miami

Building a Vertical Around Regulated Industries to Increase Your Business

Julie Machal-Fulks

Consumers of IT Services Who Are Subject to Regulatory Requirements

- Health Care Providers
- Financial Services
- Governmental agencies

Regulatory Requirements Can Extend to Managed Service Providers

- IT MSPs fall within a class of service vendors that often are required to “step into the shoes” of their customers
- When those customers are subject to privacy and data security regulations like healthcare providers, financial services firms or government agencies, MSPs must be prepared to satisfy the same regulatory requirements that apply to their customers

Compliance May Yield Dividends

- Achieving and maintaining compliance can result in a market advantage for MSPs
- Increasingly, managed services consumers either require that prospective MSPs be able to satisfy regulatory requirements
- Pro-active compliance initiatives hold the potential to open doors to new business

Major Regulatory Frameworks

- Healthcare Providers: Health Insurance Portability and Accountability Act (**HIPAA**) / Health Information Technology for Economic and Clinical Health Act (**HITECH**)
- Financial Services Firms: Gramm-Leach-Bliley Act (**GLBA**)
- Government Agencies: Federal Information Security Management Act (**FIMSA**)

HIPAA / HITECH
Overview

Health Insurance Portability and Accountability Act (HIPAA)

- Privacy and Security Rules define requirements for the appropriate use and safeguarding of protected health information (PHI)

Health Information Technology for Economic and Clinical Health (HITECH) Act

- Enacted as part of ARRA in February 2009
- Intended to strengthen the privacy and security of health information
- Applies Privacy and Security Rules to Business Associates
  - Includes breach notification requirements

HIPAA / HITECH

Are MSPs Business Associates?

The answer depends on the services provided to the Covered Entity.

- Service examples: consulting, data aggregation, management, administration, financial
- Activity examples: data analysis, processing or administration, and practice management

Covered Entities generally wish to treat most service providers as Business Associates

- If your client insists you sign a Business Associates agreement, you may be contractually obligated to comply with the HITECH breach notification requirements.

HIPAA / HITECH

Safe Harbor - Encryption

Encryption methods published by the National Institute of Standards and Technology (NIST) have been adopted by HHS

- Data at Rest – data residing in a database or file system
  - Full disk encryption (FDE) – All data on the hard drive used to boot a computer is encrypted, and access to the data is permitted only after successful authentication to the FDE product
  - Virtual Disk encryption – Encryption is applied only to a “container” file (portable) or disk volume (generally not portable), which may hold many files and folders
  - File encryption – Individual files on a storage medium are encrypted, and access is granted only after proper authentication is provided; however, file attributes and metadata may be accessible despite encryption
  - Refer to NIST Special Publication 800-111

HIPAA / HITECH

Safe Harbor - Encryption (cont)

- Data in Motion - data moving through a network, including wireless transmission
  - Transparent Layer Security (TLS) is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications
  - Security controls exist for network communications at each layer of the TCP/IP model:
    - Application Layer – Separate controls must be established for each application
    - Transport Layer – Controls at this layer can be used to protect the data in a single communication session between two hosts
    - Network Layer – Controls at this layer apply to all applications and are not application-specific
    - Data Link Layer – Controls at this layer are applied to all communications on a specific physical link and can protect both data and IP information
  - Refer to NIST Special Publication 800-52, 800-77, or other FIPS 140-2 validated means.
- **Note:** If an encryption key is leaked, information is no longer considered to be encrypted

AUDIENCE FEEDBACK

Please Rate this Session

“Building a Vertical around Regulated Industries to Increase Your Business”

1) Please TEXT one of the following codes to 22333 **(22333 acts as the phone number)**

- **60809 (Excellent)**
- **60860 (Good)**
- **60862 (Fair)**
- **60869 (Poor)**

Or, use your web browser at http://pollev.com and text in the six digit code

Or, tweet @poll and the six digit code

(Standard text messaging rates may apply depending upon your plan. Your phone number will stay private and will not be spammed).

2) Have Comments? Text 216996 and your message to 22333. Mention the session subject in your message.

Example: Text “216996 The speaker in the [subject] session gave us great insight!” to number 22333

HIPAA / HITECH

Safe Harbor - Harm Threshold

- Breach notification is required only where a breach compromises the security or privacy of PHI and that compromise poses a "significant risk of financial, reputational, or other harm to the individual."
- "Risk of Harm" factors:
  - nature of the data elements breached;
  - likelihood the information is accessible and usable;
  - likelihood that the breach may lead to harm; and,
  - ability of the entity to mitigate the risk of harm.
- The current Interim Final Rule includes this harm threshold, though there is debate as to whether it should be included in the final rule.

GLBA

Overview

- Enacted in November 1999
- Financial Privacy Rule requires financial institutions to give consumers annual notice of privacy practices
- Safeguards Rule requires financial institutions to develop written plan describing precautions taken with regard to consumers’ nonpublic, personal information
- “Financial institutions” include “companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance”

GLBA

Safeguards Rule

- Security plan adopted under Safeguards Rule must include the following elements:
  - Identification of one or more employees to coordinate the information security program
  - Identification and assessment of risks to consumer information in each area of operation, and evaluation of the effectiveness of current safeguards
  - Design and implementation of a safeguards program, with regularly monitoring and testing
  - Service-provider contracts must require vendors to maintain safeguards, and vendors' handling of consumer information must be monitored
  - Periodic evaluation and adjustment of security program in light of relevant circumstances

GLBA

Security Plan Elements

- The FTC recommends a number of elements that should be included in security plans under the Safeguards Rule. Several that may be of special significance to MSPs include:
  - Requiring employees to use “strong” passwords that must be changed on a regular basis
  - Developing policies for appropriate use and protection of mobile devices
  - Developing policies for employees who telecommute
  - Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names
  - Know where sensitive customer information is stored and store it securely
  - Taking steps to ensure the secure transmission of customer information
  - Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information
  - Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information
  - Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach

FIMSA
Overview

- Enacted in 2002
- Requires each federal agency to implement an information-security program for systems supporting the operations and assets of the agency, including those managed by contractors
- National Institute of Standards and Technology (NIST) is tasked with developing standards, guidelines, and techniques for providing adequate security for all non-DOD agency operations and assets

FISMA
Compliance Framework

- Information-security compliance framework defined by FISMA includes the following elements:
  - Information systems inventory
  - Risk-level categorization of information and systems
  - Security controls
  - Periodic risk assessment
  - System security plan
  - Certification and accreditation
  - Continuous monitoring
- Standards and guidelines for implementing the FISMA framework are defined by NIST

Pro-Active
Compliance Implementation

One of the best way for MSPs to be ready for clients who are required to comply with any of these rules is to take steps to review and implement applicable rules internally – doing so will help to familiarize team members with regulatory requirements, which can smooth the transition of responsibility for customers' IT systems

Maximizing the Value of Compliance

After implementation, use compliance to attract new work and to increase the value of the business:

- Third-party accreditation can be used to demonstrate compliance during the sales process, reducing lag time on new projects and demonstrating competitive ROI for new clients
- New IT solutions can be built or differentiated for compliance-sensitive clients, increasing the value and applicability of those solutions
- Existing clients can be made aware of new accreditations and compliance levels, which helps to maximize opportunities among managed services consumers who are already familiar with the MSP's capabilities

Questions?

Julie Machal-Fulks
Partner

Scott & Scott, LLP
1256 Main Street
Suite 200
Southlake, TX 76092
214-999-0080
julie@scottandscottllp.com

AUDIENCE FEEDBACK

Please Rate this Session

“Building a Vertical around Regulated Industries to Increase Your Business”

1) Please TEXT one of the following codes to 22333 (22333 acts as the phone number)

- 60809 (Excellent)
- 60860 (Good)
- 60862 (Fair)
- 60869 (Poor)

Or, use your web browser at http://pollev.com and text in the six digit code

Or, tweet @poll and the six digit code

(Standard text messaging rates may apply depending upon your plan. Your phone number will stay private and will not be spammed).

2) Have Comments? Text 216996 and your message to 22333. Mention the session subject in your message.

Example: Text “216996 The speaker in the [subject] session gave us great insight!” to number 22333