MeriTalk®
MeriTalk's Health IT Community

FOR IMMEDIATE RELEASE

Contact:
Christine Mulquin
(703) 883-9000 ext. 162
cmulquin@meritalk.com

82 PERCENT OF HEALTH IT EXECUTIVES REPORT THEIR ORGANIZATIONS ARE NOT PREPARED FOR THE UNEXPECTED

Security Breaches, Data Loss, and Unplanned Outages Cost U.S. Hospitals More Than $1.6B Annually

Alexandria, Va., February 3, 2014 – MeriTalk, a public-private partnership focused on improving the outcomes of health and government IT, today announced the results of its new report, "Rx: ITaaS + Trust." Healthcare IT executives agree trusted IT solutions play a key role in enabling IT-as-a-Service (ITaaS), an IT model that helps healthcare providers transform their extended IT infrastructure, improve service levels, deploy healthcare applications more quickly, and reduce costs. MeriTalk's new report, based on a survey of healthcare IT executives and underwritten by EMC Corporation, quantifies the organizational cost associated with security breaches, data loss, and unplanned outages for healthcare providers – more than $1.6B a year – and provides insight into go-forward strategies.

Health information is often a target for malicious activity and 61 percent of global healthcare organizations surveyed have experienced a security related incident in the form of a security breach, data loss, or unplanned downtime at least once in the past 12 months.

Based on estimates from health IT executives in the EMC Global IT Trust Curve Survey, these incidents cost U.S. hospitals an estimated $1.6B each year.

- *Security Breaches*: Nearly one in five (19 percent) global healthcare organizations has experienced a security breach in the last 12 months at a cost of $810,189 per incident. Health IT executives say the most common causes for breaches include malware and viruses

-more-

(58 percent); outsider attacks (42 percent); physical security – loss/theft of equipment (38 percent); and user error (35 percent)

- *Data Loss*: Nearly one in three (28 percent) global healthcare organizations has experienced data loss in the past 12 months at a total cost of $807,571 per incident. And, of those, more than a third (39 percent) have experienced 5 or more incidences of data loss in the past 12 months. Common causes of data loss include hardware failure (51 percent); loss of power (49 percent); and loss of backup power (27 percent)
- *Unplanned Outages*: Almost two out of five (40 percent) global healthcare organizations have experienced an unplanned outage in the past 12 months at a cost of $432,000 per incident. On average, healthcare organizations have lost 57 hours to unplanned downtime over the past 12 months. The most common causes of outages include hardware failure (65 percent); loss of power (49 percent); software failure (31 percent); and data corruption (24 percent)

Providers acknowledge there is more work to be done. Less than one-in-three respondents (27 percent) believe their organization is fully prepared to ensure continuous availability of ePHI during unplanned outages, disaster recovery, or emergency mode operations. And, once an emergency has passed, only 50 percent of respondents are confident in their organization's ability to restore 100 percent of the data required by SLAs. More than half (56 percent) would need eight hours or more to restore 100 percent of the data. The majority – 82 percent - say their technology infrastructure is not fully prepared for a disaster recovery incident.

Recognizing the importance of trusted IT solutions, organizations plan to focus on encryption of protected health information (55 percent); complying with the security risk analysis EMR Meaningful Use requirements (54 percent); and breach prevention and detection (44 percent).

"Healthcare organizations are making significant IT investments to transform IT infrastructure and ensure that patient information is secure, protected, and highly available," says Scott Filion, General Manager, Global Healthcare, EMC Corporation. "Trust has become a board-level business priority. Healthcare organizations have always focused on information security, but today they must do more to protect data and ensure accessibility to meet ARRA HITECH HIPPA requirements."

Of the healthcare organizations who are not currently offering a particular IT capability "as a service," half plan to do so within the next five years. Many are taking key steps to prepare – including

➢ HIPAA Security Risk Analysis as part of EMR Meaningful Use requirements	46%
➢ Single Sign On and authentication for Web-based applications and portals	44%
➢ Audit tools and log management	43%
➢ Encryption for protected health information	42%
➢ Multi-factor authentication for remote access for clinical staff accessing networks (including ePHI) remotely	35%
➢ Security analytics to help with breach prevention	32%
➢ Centralized management and authenticated access to health information	31%
➢ Data Loss Prevention to monitor the location and flow of sensitive data	29%

The MeriTalk study is based on a survey of 100 health IT executives. The EMC IT Global Trust Curve Study surveyed 283 global health IT executives.

View the video and download the complimentary "Rx: ITaaS+Trust" infographic report today at: http://www.meritalk.com/Rx.

About MeriTalk

MeriTalk is an online community and go-to resource for government and healthcare IT issues – www.meritalk.com. MeriTalk hosts a series of Exchange communities in Big Data, cloud computing, data center consolidation, and cyber security. In addition, MeriTalk develops research studies, manages events, builds applications, and routinely testifies on the Hill on IT and workforce issues.

###