Press Release

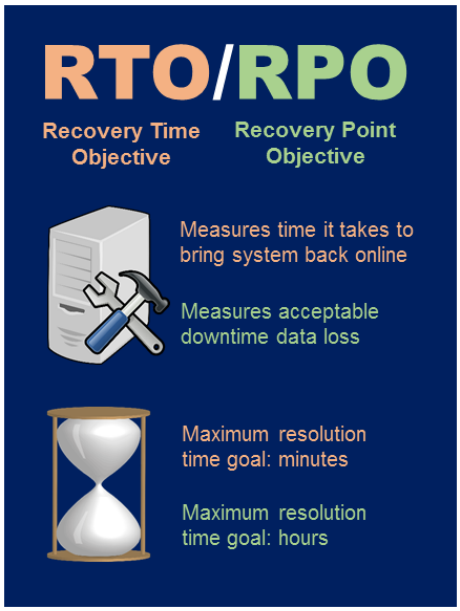
FOR IMMEDIATE RELEASE

April 14, 2016

Contact: Doug Williams
(317) 863-7676
Doug.Williams@jdrsolutions.com

CIO: A proper IT education begins with the 'two Rs'

INDIANAPOLIS – As dependable as they are, computer networks are not invulnerable to outages. When unexpected interruptions occur it is important to know how fast offline systems can be back up and running, and the maximum data-losing downtime that is acceptable.



Those two factors, known as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), respectively, sound almost synonymous in name and definition, but they are quite different, said Doug Williams, Chief Information Officer for JDR Solutions Inc. (www.jdrsolutions.com), an Indianapolis-based provider of software and portfolio management services to the equipment leasing industry.

"You run a real risk of significant data loss if you don't know your system's RTO and RPO during outages, and have a response plan in place," Williams said. "That becomes especially critical if your company hosts data for another business, particularly in the cloud. Having a solid RTO/RPO plan could mean the difference between business survival and failure."

While RTO and RPO times can vary depending on the company and the mission-critical nature of its network, the best RTO plans call for resumption of service within minutes. Ideally, no RPO should extend beyond a few hours.

In this age of round-the-clock access to computer networks, a company can ill afford a long downtime. As offline time increases so, too, does the risk of data loss.

IT professionals should continually strive to shorten both RTO and RPO times, Williams said.

"At JDR Solutions we've made a commitment to reducing RTO and RPO," Williams said. "Our numbers show we've made great strides over the years. Our service level agreement goal is for RTO to be 15 minutes with zero data loss. Within our industry that is phenomenal."

JDR stores the lease portfolio data it manages for clients on cloud servers located in multiple U.S. locations. The company also maintains relationships with several international cloud service providers. Utilizing out-of-state, or even out-of-country, cloud providers ensures greater data protection should a technological or natural disaster render the cloud customer's systems inoperable, Williams said.

So how does a company address RTO and RPO concerns? Regular operational audits like those conducted as part of the International Organization for Standardization (ISO), Occupational Health and Safety Management Systems (OHSMS), International Technology Infrastructure Library (ITIL), Service Organization Control (SOC) and Payment Card Industry (PCI) programs are a good place to start. Companies designated complaint with those programs meet the highest standards of operational excellence.

Educating employees and customers on data storage and retrieval best practices also helps.

"When a client sends a file to a vendor the client can check with the vendor to make sure that file was received," Williams said. "If the vendor doesn't acknowledge receiving the file the client can resend and try contacting the vendor again. On the other side, the vendor can verify communications with the client's server. If the client's server is running the vendor should receive notification. If not, the vendor can send out tech support."

Overall, IT professionals must remain vigilant.

"You've got to stay on top of things and prepare for outages that will happen," Williams said.

NOTE TO MEDIA: For a publication-quality version of the graphic and additional information and interviews, contact Steve Leer, JDR's director of marketing, at (317) 863-7664, or Steve.Leer@jdrsolutions.com.

###