Roundtable: Technology Offers Proactive And Defensive Solutions

The Editor interviews ***Jon Resnick****, Worldwide Vice President of Field Operations and Marketing at Applied Discovery;* ***Thomas J. Svoboda****, Managing Director, Marketing and Education at Evidence Exchange; and* ***Scott Giordano****, Corporate Technology Counsel at Mitratech.*

Editor: The *New York Times* recently reported that the Internet – including the cloud and social media – has become a dangerous place. Do you agree?

Resnick: Yes, the Internet can be downright deadly if your company does not have the proper policies and protocols in place to ensure that your data is protected. As we have learned from countless social media scandals this year, including Weinergate, as soon as the information escapes your keyboard, it is published forever in the Internet's annals. We have also learned that no one is immune from potential data breaches from the almost-weekly, high-profile breaches that have affected millions of consumers' data, including those at Epsilon, Sony, Citibank, ADP, the International Monetary Fund and Congress.

However, that does not mean we need to retreat from the Internet: we just need to be more vigilant. Specifically, companies must develop sound policies and standards governing the use, dissemination and storage of electronically stored information (ESI) in every format. As Joshua Kubicki, our Director for Legal and Corporate Practices, wrote in "Risks And Rewards: The Wild West of Social Media," (http://www.metrocorpcounsel.com/current.php?artType=view&EntryNo=12427) creating a social media policy is critical. In doing so, you will need to figure out how restrictive your policy should be, to train your employees on the terms of the policy and to enforce it.

Additionally, Keith E. Moore, our V.P. of Technology Solutions, suggests in "Don't Let A Data Breach Turn Your Case Into A Bet-The-Company Matter" (http://www.metrocorpcounsel.com/current.php?artType=view&EntryNo=12009) that cloud computing can be perfectly secure, so long as companies work with service providers to institute best practices. In particular, companies should ensure that security procedures are documented in the service agreement, including managing data using a chain of custody log; controlling access to data; auditing network and user transactions; using a virtual private network; and employing intrusion detection and prevention systems. Putting protocols such as these in place will dramatically increase the safety of a company's data.

Svoboda: No. Whether hardware and software exists in the cloud or in your own data center, technology platforms have never been more stable or more reliable. While no system is immune from failure, outages like the one mentioned in the *New York Times* article are extremely rare. However, before entering the cloud, you must assess the work you do and then develop an orderly implementation plan. For the most part, there are three types of work.

First, certain applications will be obvious candidates for the cloud, and savvy users will immediately recognize them. They will begin moving those applications to the cloud, and as a result, successful enterprises will quickly gain the benefits. Second, certain mission-critical applications, which you have worked hard to optimize, should remain in their current operating environment. It makes no business sense to take any risk with these all-important applications. So, for now, leave them be. Third, special applications that may require highly intensive computing, such as analytics or applications that require very large input/output devices, are good candidates for the cloud. This may be work you previously thought would not be possible due to cost and technology requirements.

Cloud computing is a new model of consuming and delivering IT and business services. It enables users to get what they need, as they need it – from advanced analytics and business applications to IT infrastructure and platform services, including virtual servers and storage. It can provide significant economies of scale and greater business agility, while accelerating the pace of innovation.

The cloud gives you more options for deploying applications. Not only can you achieve great savings, but also you can increase the reliability of your overall IT operation. So, in many respects the cloud can help reduce the "danger" resulting from catastrophic system failures. The cloud is secure, efficient and scalable.

Giordano: The Internet has become a potentially dangerous place for corporate legal departments. Early on in the adoption of the Internet by those departments, the dangers were mostly related to the security of documents stored in Internet-accessible places and to communications privacy. As the public's use of the Internet has spread, the danger has grown to include reputational damage from statements made by company employees on social media sites or even loss of trade secret status for information that leaks out of the company network or that of a cloud service provider.

However, corporate legal has benefited greatly from Internet access, enabling rapid communication and collaboration worldwide and speeding legal research and document construction. In order to continue enjoying those benefits, department and IT leaders can adopt three particularly cost-effective security strategies: administrative policies, role-based access control or RBAC, and business rules. Administrative policies include conducting thorough background checks of prospective employees, contractors and business partners; requiring employees to acknowledge what constitutes acceptable use of e-mail and the Internet; and requiring two people to authorize certain actions, such as issuing payments. RBAC is a technical security measure that works by allowing employees to access information based on their roles – a general counsel will have greater access than staff counsel, who will in turn have greater access than a paralegal. Business rules allow the department to set a fail-safe rule – e.g., to obscure any part of an electronic document that has a social security number or date of birth – if the person viewing is not part of a designated "need to know" group. Modern enterprise legal management systems either include or support all of these security measures while enabling legal team members to collaborate and promote the company's mission. With these measures in place, the Internet offers legal far more promise than peril.

Editor: What are the emerging legal and business needs that eDiscovery and data security product solutions must address? Is technology keeping pace?

Resnick: Two major needs: security and efficiency. Each day, we read about cybersecurity threats and data breaches that cost companies millions of dollars in lost information. The Ponemon Institute's Second Annual Cost of Cyber Crime study revealed a 56 percent increase in the annualized cost of computer crime from last year, with a median cost of $5.9 million. The study warns companies that cyberattacks are inevitable, whether by viruses, worms, trojans, malware or botnets. One way to protect companies against these types of attacks is to obtain a cyberinsurance policy, which can cover the cost of lost business and data as well as offer privacy and security liability coverage.

In addition, the mind-boggling volume of ESI that companies create and retain renders it nearly impossible to review all data manually due to prohibitive deadlines and costs. Fortunately, technology can ease the pain and cost of manual review. For example, as United States Magistrate Judge Andrew J. Peck of the Southern District of New York declared at July's Carmel Valley eDiscovery Retreat, 2011 is the year of predictive tagging. Using this technology, review teams code a core sample set of documents, and then the technology engine analyzes those tagging decisions along with the documents' content characteristics and applies the logic across the entire data set. Thus, the most relevant documents are quickly grouped for prioritized, contextual review, yielding dramatically improved results from keyword searches.

In addition, eDiscovery providers are offering services that make it simple to outsource projects. For example, managed review services offer traditional document review as well as consulting, data mapping and analysis, sampling data, interviewing custodians, organizing and training review teams, budgeting, and the like. In other words, these services compose a comprehensive eDiscovery package that combines review expertise and project management to save clients time and money.