

Peer to Peer

Risky Business



Peer to Peer March 2010

Bridging the “Risk-Speak” Language Barrier

YURI FRAYMAN AND KANDACE DONOVAN **THE FRAYMAN GROUP**

When legal IT staff and partners try to communicate, it often seems like they are speaking different languages. One topic especially leads to dangerous translation errors — security. Poor security equals risk to the business. This is understood on both sides, but how do you define security, and how do you define risk?

As legal IT professionals, you are entrusted with ensuring the security and integrity of the systems and data the firm relies on. You’ve tightly locked down your firewall, applications and databases. You’ve trained your users to practice “safe computing” by selecting secure passwords and avoiding suspicious attachments to e-mail messages. You’ve examined the network for vulnerabilities and configured a disaster recovery system. You’ve thought about both intentional and unintentional actions that can put the systems you are responsible for at risk. You’re feeling pretty good about the work you’ve done, and rightly so. So why do the partners keep talking about risk?

The security of the business, and how to remove risk from the business, are completely different topics that refer to very different things. Whether you’re a firm of one lawyer or 10,000 lawyers, your business will have security risks. Someone needs to be thinking every day about the security of the business, not just the security

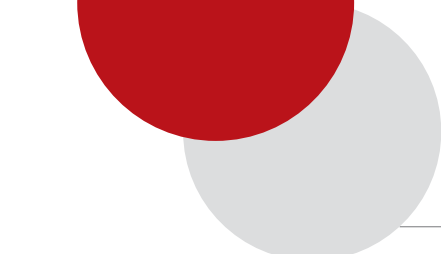
of the business systems. You can help reduce that risk, if you’re speaking the same language.

BROADEN YOUR VIEWPOINT

Here are some questions partners might ask when thinking about security and risk concerns:

- Are we taking on the right business, and are we properly balancing intake speed with the minimizing of risks?
- Are we protecting ourselves from accusations of impropriety, and can we prove it?
- Can we properly manage the increased number of lateral hires we are taking on?
- Are we going to get paid for the work we do?
- Can we eliminate manual errors in our highest risk business processes?
- Will senior partners be alerted of irregular activity within the firm before it’s too late?

The stakes on this side of the table are many times higher than the consequences of being infected with a computer



virus or failing to implement proper password policies. Firms can face heavy fines from authorities when they ignore their business risks, or the firms can disappear altogether. Of course, any mishandled situation has the opportunity to become an embarrassment and can damage the firm's ability to attract new business.

An end-to-end risk management solution requires well thought-out processes and a good risk management system, both of which the savvy IT professional can influence.

TWO SIMPLE STEPS TO A MORE SECURE FIRM

First, understand the connected business processes that govern the major stages of risk management. These include the following:

- **Taking on new business**
- **Hiring laterals**
- **Checking conflicts**
- **Building and maintaining ethical walls**
- **Managing legal holds**
- **Monitoring improper use of firm intellectual property and systems**

These critical business processes represent the primary challenges facing today's law firms: the competitive importance of speed to new business, continued uptick in lateral acquisitions and mergers, risk profile management, and compliance with ethics rules and regulations, all of which need to be addressed while efficiently and profitably managing the business.

Knowledgeable IT professionals can exert considerable influence over selecting the right risk management approach and the right system. Rather than following the outdated approach of tackling each problem in a silo — where one product does conflict checking, another handles new business intake, and still another enables ethical wall creation — business-savvy IT leadership can demonstrate value to the firm by taking the initiative and tackling the problem holistically.

A holistic approach reaps many benefits in that one system equals one version of the truth. This minimizes manual errors between steps of the process and eases auditability. In sum, a holistic approach minimizes both the technology and the business risks facing firms today.

UNDERSTAND WHAT IS AT STAKE

Law firms are required to secure and control access to "sensitive" information under their care. Information can be deemed sensitive and require safeguarding for ethical or privacy reasons as defined by the firm itself, its clients, guidelines and regulatory requirements or the courts. Securing information access across all firm personnel, offices and technology systems is no easy task. Traditional approaches that rely on fee earners and support staff to enforce confidentiality are no longer sufficient to satisfy clients' needs and regulatory requirements.

For example, a simple error in transposing a name from a conflicts tool to an ethical wall tool could have huge negative repercussions for the firm. Not only could such a mistake lead to major embarrassment for the firm, possibly in a very public forum, but also the firm could be disqualified from the case. A "disqual" can result in severe financial implications for the firm: lost revenue, government penalties and significant damage to the firm's reputation. A recent conservative estimate of the cost of disqualifications is an annual price tag of more than US\$65 million.

While an error like the above introduces risk to the business unintentionally, a business-minded IT professional must also protect the firm against potential intentional harm. This means being able to alert senior partners immediately to the irregular activity of one of the firm's staff — not just detecting access of a large number of documents in a short period of time, but intelligently distinguishing between patterns of day-to-day activity across systems and truly atypical behavior. Will your system automatically halt attempts to manually reverse security established by the ethical walls system? The firm's intellectual property is second in value only to one thing, the firm's reputation. And both are at risk if the answer is no.

BECOME BILINGUAL

When it comes to security, the legal IT department is responsible for protecting the firm from various external threats such as viruses, hackers and the like. They also manage passwords and encryption systems to ensure internal security. However, when it comes to risk management, IT professionals will benefit from demonstrating why the security is in place rather than focusing only on maintaining siloed risk management tools.

By seeing risk management tools as separate entities, you could possibly jeopardize the firm. However, by speaking both languages and understanding how the business side of risk informs IT, and how the technology in turn impacts business, you can take steps to ensure security with your risk management platform across all of its components. You can move toward a comprehensive, end-to-end risk management solution that provides all parties peace of mind. **ILTA**



Yuri Frayman is President and CEO of The Frayman Group. He has over 20 years of experience in providing mission-critical solutions to the global legal market. Yuri previously founded LegalKEY Technologies Inc. He can be reached at yfrayman@fraymangroup.com.



Kandace Donovan is Senior Vice President and General Manager, North America, of The Frayman Group. She has more than 20 years of strategic leadership and business development expertise and has consulted with more than 250 law firms about their risk management needs, helping them to select and implement solutions to improve their businesses. She can be reached at kdonovan@fraymangroup.com.