

Balancing Transparent Access to KM with Client Security, Confidentiality, Risk and Compliance

#INFO14

August 25, 2011

Speakers

Dave Cunningham

Managing Director

HBR Consulting (formerly Hildebrandt Baker Robbins)

Browning Marean

*Senior Counsel & Co-Chair of the firm's Electronic Discovery
Readiness and Response Group*

DLA Piper

Jennifer Minicucci

Director, Information Risk and Compliance

Patton Boggs LLP

Agenda

- **From whom are we protecting?**
- **What information needs to be protected?**
- **How do firms protect this information?**
 - *Standard tools and procedures*
 - *Emerging tools and procedures*
- **Beyond these forms of protection, how can firms lessen the chances that insiders will use firm data for improper purposes?**



From whom are knowledge managers protecting data?

- **Internal**
 - Employees with insider trading intentions
 - Employees who accidentally see confidential data
 - Employees who re-use content outside their expertise
- **External**
 - Clients and third parties who may accidentally be sent confidential information

What information may be useful to insiders?

- Document names and descriptions
- Precedents
- Active material
- Litigation support data
- Conflicts
- New business intake
- Time entry
- Extranet sites
- Verbal discussions
- Records data
- Newsletters and status reports
- Physical war rooms
- Travel agendas
- Legal project management systems

How do firms protect this information?

Standard Tools

- Ethical walls for known sensitive matters
- Project code names
- Enterprise searching that recognizes folder and file security
- Password protection for documents and spreadsheets
- Locking and wiping of remote access devices; security software on remote device
- Minimum password sophistication
- Required screen saver usage
- Two-factor authentication
- Account auditing / monitoring

How do firms protect this information?

Emerging Tools

- Document naming standards
- Matters secured by default / ethical walls for all matters
- Knowledge Management as gatekeeper
- Third party agreements and procedures
- Identity management
- Monitoring for unusual activity (users and IT)
- Encryption (data in transit / data at rest)
- Intelligent redaction software
- *Audience Suggestions?*



How else can we protect firm data from improper access & use?

- Policies
- Ethical training and reinforcement

Questions?

- Dave Cunningham
dcunningham@hbrconsulting.com
- Browning Marean
Browning.Marean@dlapiper.com
- Jennifer Minicucci
JMinicucci@PattonBoggs.com

Selected Articles

Block, Meg & David Cunningham. “Legal Information Risk – Action Plan and Roadmap,” *Peer to Peer*, June 2011.

<http://www.mygazines.com/issue/34686/33>

Harbert, Tam. “Catch Me If You Can,” *Law Technology News*, June 1, 2011.

<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202494769505&slreturn=1&hbxlogin=1>

Nelson, Sharon. “Your Chance of Being Hacked in Twelve Months Now a ‘Statistical Certainty,’” *Ride The Lightning Electronic Evidence Blog*, June 30, 2011.

<http://ridethelightning.senseient.com/2011/06/your-chance-of-being-hacked-in-twelve-months-now-a-statistical-certainty.html>

Selected Resources

Law Firm Risk Resources (short list from 2009).

<http://lawfirmriskresources.wikispaces.com/>

Law Firm Risk Management Blog.

<http://www.lawfirmrisk.com/>

InfoRiskAwareness Blog (UK focus).

http://inforiskawareness.co.uk/best_practice/

Hildebrandt Baker Robbins Blog (selected posts).

<http://info.hbrconsulting.com/blog/archive/2011/06/01/balancing-information-security-and-collaboration-a-knowledge-management-view.aspx> and

<http://info.hbrconsulting.com/blog/archive/2011/05/13/risk-management-at-law-firms-a-rapidly-evolving-issue.aspx>