RATIONAL Enterprise

Bringing Rationality to Information Management

Dear Trusted Advisor, Are You Really That Trustworthy?

Law firms and other advisory firms are entrusted with a client's most sensitive data – data that includes personally identifiable information (PII), trade secrets and other intellectual property (IP), and confidential and privileged information. Moreover, these very same firms are advising their clients on best practices for securing such data. Yet, these advisors are storing client data in risky locations with inadequate security, unnecessarily exposing it to inadvertent disclosure. This situation may subject these trusted advisors to increased liability. Trusted advisors should consider taking measures to practice what they preach.

Security breaches are an ever-present and increasing concern to top-level executives, yet seem to be an unavoidable consequence of today's connected world. If there is one group that is simultaneously the most trusted custodian of sensitive data, the most likely to be hacked, and the most ill-equipped to handle an attack or intrusion, it is law firms and other consulting firms – the very firms that advise their clients on cyber security and therefore ought to know better.

Law firms and consulting firms expose themselves to the largest information security risk due to the nature of the data with which they are entrusted. These trusted advisors hold some of the most valuable client data – personal employee data, intellectual property, financial information, confidential and privileged information – yet they store that data in some of the most risky locations (e.g., personal computers, where most work product is produced). Even with baseline security measures on risky storage devices, advisors are unnecessarily making themselves vulnerable to significant liabilities from data breaches. This shortcoming is especially problematic as these law firms and consulting firms are often in the business of advising their clients on how to mitigate risk by better managing and protecting data in the context of compliance, information technology, and litigation. However, the very nature of the work that these firms perform – advising their clients on information privacy and security processes and technology – only increases their duty to protect client data. Trusted advisors must begin practicing what they preach. Smarter information governance is the answer.

Rational Enterprise offers trusted advisors the ability to mitigate information security risk with software that provides in-place and real-time visibility into and management of all unstructured data. This level of insight and control, combined with automated, content-based classification of the data, enhances cyber security protections in several important ways:

1. Rational can proactively defend against cyber security threats by identifying sensitive data and moving it to the most secure storage locations.

2. Rational can improve baseline security by attaching document classifications to each document so that the existing security infrastructure can be informed by it. These tags allow existing data loss prevention (DLP) tools, firewalls, email gateways, proxy servers, etc. to leverage sophisticated document classification to identify and protect the most sensitive documents, while allowing lower risk documents to pass without interruption.
3. Rational can similarly enhance the capabilities of an information security monitoring system by allowing it to leverage content classification to better detect threats proactively and improve response protocols.
4. Rational can provide definitive answers to the troubling questions that arise following a data breach, like “what is our exposure?”