

## CREDANT Mobile Guardian

Responsible Management of Endpoint Data Security for Law Firms



### REGULATORY OVERVIEW

Data protection or lack thereof, makes headlines. Yet for law firms, data security can be particularly tricky.

Mandates concerning discovery and disclosure in legal cases, such as the United States Federal Rules of Civil Procedure (FRCP), define rules for quickly finding and disclosing relevant information. Data security can't interfere.

Yet the variety of places where data can be compromised is increasing. As reported in the 2008 American Bar Association Legal Technology Survey:

- › Use of laptop computers vs. desktop models jumped 14% from 2007 to 2008
- › In 2008, 76% of respondents reported the availability of smart phones or BlackBerrys at their firms, up from 55% in the 2007 survey and 49% in the 2006 survey.
- › 8% of respondents report that their firms have experienced a security breach

Even with this growth in potential points of data breach, few if any State Bar Associations mandate specific data protection or privacy schemas. And yet, state and federal laws impose hefty penalties, liabilities, sanctions, and even imprisonment of legal firm management when sensitive information is compromised under the wrong circumstances.

So it's not surprising that most legal firms try to establish horizontal data security practices that address a broad range of client needs. These best practices enable IT managers to:

- › Establish IT best practices for assessing risks across all data storage elements (e.g. laptops and USB sticks used as lawyers travel)
- › Devise documentation that illustrates compliance to a wide range of mandates
- › Educate employees on data security
- › Devise means for security to be user-friendly regardless of how tech savvy they are (or aren't)
- › Schedule and run regular security audits with an eye to being ready at a moment's notice should a client firm be audited
- › Regularly test that data secured is easily retrievable should it be required for legal discovery or disclosure

### CREDANT SOLUTION

*CREDANT encryption management solutions ensure that encryption and security mandates are consistently and efficiently enforced –regardless of where the data resides.*

#### ONLY CREDANT ENABLES ORGANIZATIONS TO:

- › Manage encryption and secure data across multiple endpoints from a common management platform
  - › Full Disk Encryption (FDE)
  - › Self-Encrypting Drives
  - › Policy-Based File/Folder Encryption
  - › Mobile Devices and Smartphones
  - › Removable Media
  - › Windows<sup>®</sup> BitLocker<sup>™</sup>
- › Create automatic audit trails that offer proof of end-to-end data security
- › Provide a transparent end-user interface that supports user productivity while keeping data safe
- › CREDANT provides you with a centrally-managed, highly scalable and architecturally flexible approach to manage all data endpoints. With CREDANT, organizations can:
  - › Help ensure data security, reducing the risk of insider or external attack
  - › Simplify and reduce the workload of maintaining compliance
  - › Provide confidentiality, privacy and auditing of data residing on any endpoint
  - › Integrate and manage multiple encryption solutions into a single management tool set

## CREDANT Mobile Guardian

Responsible Management of Endpoint Data Security for Law Firms



### LEGISLATION AND REGULATION

Following is a snapshot of regulations impacting law firms today:

#### US FEDERAL RULES OF CIVIL PROCEDURE (FRCP)

FRCP affects every business, organization, and person who may ever be involved in a federal court case. Such cases include law suits that cross state lines, actions by the Internal Revenue Service, and violations of federal compliance regulations (such as HIPAA and Sarbanes-Oxley), immigration cases, and more. Heavy fines and non-monetary sanctions are in play if “electronically stored information” is not disclosed as mandated. FRCP also places a time limit for disclosure and stipulates retention schedules, including rules for when or how emails may be deleted.

#### HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

First described in 1996, the final HIPAA standards rules was published in 2003. HIPAA identifies a series of security procedures to assure the confidentiality of electronic health information. These procedures include administrative, technical and physical measures. Along with detailed security rules, HIPAA includes provisions to investigate complaints, collect information and determine a covered entity’s compliance.

#### GRAMM-LEACH-BLILEY ACT (GLBA)

Under GLBA, the Federal Trade Commission (FTC) has Safeguards that require implementing security measures to protect “customer information” —information such as names, addresses, account and credit information, and Social Security numbers. The FTC Safeguards cover both integrity as well as protection against unauthorized access to or use of such records. To attain a consent order from the FTC, a company must retain an independent professional to certify, within 180 days, that its information security program meets the standards listed in the order and also to make this certification every other year for ten years.

#### SARBANES-OXLEY ACT OF 2002

While not restricted to the legal industry, the Sarbanes-Oxley Act applies to all publicly traded firms, including law firms and their

clients, by the end of 2009. Section 404 requires publicly owned companies to include both a management report and an auditor report on the effectiveness of its internal controls over financial reporting (ICOFR) within its annual report. It also requires “full, fair, accurate, timely, and understandable disclosure,” making executives and financial officers personally responsible for audit requirements and timely reporting demands

#### THE CALIFORNIA LAW ON NOTIFICATION OF SECURITY BREACH (SB 1386)

The California Law on Notification of Security Breach (SB 1386) relates more to disclosing a security breach vs. the security of the data itself. Notification could be delayed if there is a legitimate law enforcement agency determined that giving notice to the data subject would impede a criminal investigation. Notice may also be delayed if the organization suffering the breach is taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system. Over 30 States have passed similar legislation.

#### THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCIDSS)

If your legal firm takes credit cards for payment, then you is subject to the Payment Card Industry Data Security Standard (PCIDSS). The PCIDSS requires that all “merchants” accepting credit cards comply with a number of technical, physical, and administrative requirements. Failure to comply with the PCIDSS could result in large penalties and suspension of the right to use credit cards for payment purposes.

### CREDANT

CREDANT is the Trusted Expert in Data Protection. Founded in 2001, CREDANT enables organizations to control, manage and protect data on vulnerable laptops, desktops, PCs, Macs, smartphones and removable media devices. Protecting sensitive information on more than 7 million endpoints at over 1,000 global customers, CREDANT provides the most comprehensive mobile data protection and management platform.

For more information, visit [www.credant.com](http://www.credant.com).