# IT Risk Management in the Law Firm

## Protecting Client's Confidential Information

DataGuardZ White Paper

# IT Risk Management in the Law Firm

## Do you know how valuable the information is within your law office?

Lawyers deal with more confidential and privileged information than any other professionals. As a group, lawyers deal in more commercially valuable secrets than most professions, making law firms and law departments attractive targets for sources, including externally from hackers, cybercriminals, economic spies or dishonest adverse parties, and internally from trusted insiders, including staff members.

Lawyers give advice about proprietary information and other secrets and need to establish a risk management process in connection with that advice. Lawyers have explicit ethical rules, particularly rules relating to competence and confidentiality, that makes risk management essential to their profession.

## Lawyer's Professional - Ethical Responsibility & IT Risk Management

Lawyers are required to practice law in compliance with the requirements of professional responsibility embodied in the version of the Model Rules or the Model Code adopted by the jurisdictions in which they are licensed. Lawyers who maintain electronic information in their practice will have to deal with IT Risk Management thereby identifying anticipated threats to the information assets, including an inventory of information assets to determine what needs to be protected. The next step is development and implementation of a comprehensive information security program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks.

Although IT Risk Management may seem a technical matter, lawyers have a duty to implement risk and control processes ensuring that threats and vulnerabilities of the client's data are routinely identified and assessed followed by the execution of an effective risk mitigation plan. Failure to do so could result in violation of a lawyer's responsibilities under the Model Rules of ProfessionalConduct.

("Model Rules") or the Model Code ("Model Code") of Professional Responsibility.

## Model Rules of Professional Conduct Client-Lawyer Relationship

## Rule 1.6 Confidentiality of Information

A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information (deliberately or non-deliberately) relating to the representation. This contributes to the trust that is the hallmark of the client-lawyer relationship.

## Model Rules of Professional Conduct Acting Competently to Preserve Confidentiality

## Rules 1.1, 5.1 and 5.3

A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure. When collecting, processing, using, storing, transmitting or destroying information in its entire lifecycle relating to the representation of a client, the lawyer must take

reasonable precautions to prevent the information from coming into the hands of unintended recipients. In some jurisdictions, the inadvertent disclosure of confidential information could result in loss of its protected status.

The duty to protect a client's confidences clearly implicates the confidentiality, integrity and availability (CIA) component of information security. Law partners must take reasonable steps to ensure that the electronic information processed, stored and transmitted on the systems implemented in the law office is adequately protected from unauthorized disclosure. Failure to do so could run afoul of the requirement to protect the confidences of a client and result in jeopardy to the protected status of a lawyer's work product.

## Arizona Bar Opinion expanded into other states!

The Arizona Bar Opinion was first to assert that in order to meet her ethical obligations, an attorney or law firm must "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." It also requires attorneys to take competent and reasonable steps to ensure that "the client's electronic information is not lost or destroyed." The Opinion states that in order to ensure that this "competent and reasonable" standard is met, an attorney or law firm must possess the technical expertise necessary to competently "evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software."

Recognizing that few practicing attorneys possess the expertise necessary to effectively implement computer security measures, the Committee asserts that an attorney who does not possess the expertise is ethically required to retain an expert who does have such competence.

The ABA House of Delegates adopted changes to the Model Rules of Professional Conduct dealing with the question of whether and how lawyers might deal with "confidentiality issues arising from technology." The changes were suggested by the ABA Commission on Ethics 20/20 and were, "designed to give lawyers more guidance regarding their confidentiality- related obligations when using technology."

Other State Bar Associations have followed suit and issued formal ethics opinions regarding lawyers responsibility in using technology while ensuring confidentiality, including:

- State Bar of California Standing Committee on Professional Responsibility and Conduct: Formal Opinion 2012-184
- Massachusetts Bar Association Ethics Opinion 12-03
- Oregon State Bar Association Formal Ethics Opinion Number 2011-188: "Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials"
- North Carolina State Bar Association Proposed 2011 Formal Ethics Opinion 6: "Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (10/20/11)
- Iowa State Bar Association Committee on Ethics and Practice Guidelines: Ethics Opinion 11-01: "Use of Software as a Service – Cloud Computing" (9/9/11)
- State Bar of California Standing Committee on Professional Responsibility and Conduct: Formal Opinion 2010-179 (2010)

- New York State Bar Association Committee on Professional Ethics: Opinion 842 (9/10/10)
- Maine State Bar Professional Ethics Commission: "Client Confidences: Confidential firm data held electronically and handled by technicians for third-party vendors;" Opinion 194 (6/30/08)
- New Jersey Bar Advisory Committee on Professional Ethics: "Electronic Storage and Access of Client Files;" Opinion 701 (4/24/06)

## The Various Consequences of a Breach of Confidential Information:

*Discipline:*
Violation of a state disciplinary rule can result in disciplinary actions with grave financial and social consequences, such as temporary suspension or permanent disbarment from the practice of law, in addition to fines, restitution of ill-gotten gains, and mandatory pro bono service. A grievance can theoretically be brought even if a client has not suffered harm.

*Waiver of Attorney-Client Privilege*
Stated simply, the attorney-client privilege is an evidentiary rule that allows a client to refuse to disclose, and to prevent others from disclosing confidential communications between the client and an attorney (and representatives of each).

*Malpractice Liability:*
Monetary damages can be imposed on lawyers who breach a duty to their clients that causes harm. In addition, even absent harm, a client can seek return of fees paid to a lawyer if the lawyer has breached a duty to the client. These claims can come in the form of tort, breach of contract, fraud, or breach of fiduciary claims. A malpractice claim could be based upon inadvertent breach of confidentiality. The key issue is often whether the attorney met the requisite professional standards of skill and care. A jury will likely be instructed to impose liability for a claim of breach of confidentiality if the lawyer did not comply with Model Rule 1.6.

*Loss of client confidence:*
Confidential client information is the lifeblood of a legal practice and the value that the law office is able to generate for its clients is directly related to its ability to process data confidentially, accurately, and efficiently. Moreover, because the client information entrusted to the lawyer is highly sensitive and valuable, assuring the security of these data is a core customer trust and relationship issue. Conversely, breaches or potential compromises of data security – and any failure forthrightly and comprehensively to respond – can quickly undermine or destroy that trust. The publicity alone can have a devastating aftershock. Confidential information that is misused is seen within any industry as poor business process and loss of consumer confidence is most likely evident.

*Data Breach Notification Laws*
Now consider that while you may have the same devastating business loss as you suffered above, with a data breach, your law office may now have additional and expensive responsibilities. If the data that was lost is considered confidential and consumer related, it is considered a Security Data Breach which may require your law office to conform to any number of Data Breach Notification Laws or risk federal or state

penalties. A security breach can be very expensive including client notification process and credit monitoring, loss of current and future business, lawsuits and fines can increase to unrecoverable amounts.

## What Must Lawyers do to Upheld Their Responsibilities?

Lawyers must ensure that confidential, privileged, or private client information within the lawyer's possession or control is reasonably secure against inadvertent or unauthorized disclosure, alteration, and destruction. The lawyer must exercise professional diligence in managing the use of technology to ensure client information security and protection of confidential client information.

## What do clients expect from Law Firms?

With the pervasiveness of electronically stored information, a new paradigm of providing data privacy protections has emerged. Clients are asking their lawyers to produce the firm's written comprehensive IT Risk Management plan in accordance with the clients' applicable regulatory compliance requirements. Law firms have clients who must comply with regulations like the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, and the Payment Card Industry Data Security Standards, to name a few. When protected data is transferred to the law firm by the client, the law firm must also comply with these regulations and provide adequate safeguards.

## How can DataGuardZ help you control the potential risks that threat your client's confidential data?

DataGuardZ provides services which help Law Firms comply with Model Rules requirements by assessing the existence and/or effectiveness of controls required by the regulators. Our competent staff will provide a report focusing on the non-compliance with the Model Rules, we then suggest a cost effective action plan which would mitigate risks while also satisfying the regulators by demonstrating management's goodwill and due diligence in managing IT risk.