The emergence of data analysis, cloud computing and other Information Age technologies has been a boon for the legal industry. Yet the sheer amount of data being generated today is staggering. An IBM study revealed that we create 2.5 quintillion bytes of data on a daily basis, and nearly 90 percent of all existing data was created in just the last two years. Given the size of these numbers, the ability to effectively secure sensitive information has never been more critically important, or more challenging.

In this landscape, it’s no surprise that data breaches grow more numerous with each passing year. Bloomberg recently reported that 2016 was a record year for security breaches, with the total number of incidents increasing 40 percent over 2015. In one notable episode, a Russian hacker was able to extract the confidential client files of 50 law firms.

Such lapses are costly. According to the Aon Corporation the average cost of a data breach is $217 per compromised file. It’s also important to realize that not every breach is the result of criminal activity. The Aon Corporation also reports that more than half of all privacy breaches are the result of employee or system error.

The cumulative effect of these intrusions and lapses has been acutely felt by the legal industry. Recent surveys show that two-thirds of Chief Legal Officers and General Counsels rate information privacy and data security as being “very” or “extremely” important. That same survey showed that the number of these executives rating these priorities as “extremely important” has risen by more than a third since 2014.

**MODEL INFORMATION PROTECTION AND SECURITY CONTROLS**

Developed for in-house counsel, the ACC (Association of Corporate Counsel) Model Information Protection and Security Controls, which was announced in March 2017, is intended to serve as a benchmark for outside counsel and their vendors’ information security practices providing services to corporate legal departments. It offers 13 guidelines (called model controls) covering areas such as data management, threat protection and employee/contractor screening.
These guidelines help firms to implement a “Defense in Depth” strategy as pioneered by the National Security Agency (NSA). The idea is to have multiple layers of security defense and not to rely on only one approach (see Figure 1).

**Increased Scrutiny for Law Firms**

With the threat of more Information security attacks, it has become increasingly common for in-house counsel, especially those in highly-regulated areas such as finance, to audit their law firms to test the strength of their data security defenses. Law firms that fail to meet these security standards or vendor management guidelines are at greater risk of losing business.

Given the critical nature of protecting their clients’ sensitive data, many law firms would benefit from a comprehensive information security program designed to meet modern security threats, whether internal, external or from a third-party vendor. The adoption of the ACC Model Information Protection and Security Controls is one answer to help protect your clients’ information.

**UNDERSTANDING THE BASICS**

Before covering the ACC Model, it’s important to understand the core distinction between information security and cybersecurity. While these terms are often used interchangeably, cybersecurity entails the protection of data within electronic environments—protecting a computer from malicious attack, for example.

Information security is a broader concept that addresses the protection of data in all its forms, whether electronic or physical. It includes cybersecurity as one component, but has a larger mandate to safely manage data wherever it may be found. Consider the example of physical records kept in an unsecured filing cabinet, or old documents that were insufficiently shredded, then left in the trash.

**HOW THE ACC MODEL BUILDS UPON EXISTING SECURITY POLICIES**

It is standard for most law firms to have an information security policy. Yet the truth is that simply having a policy in effect offers little protection against the rising likelihood of a data breach. Many policies are either too limited in scope, too out-of-date or simply not designed to deal with the reality of modern data protection. According to the 2016 American Bar Association technology survey, only 17 percent of law firms have an incident response plan in place to address a breach—a number that rises to 50 percent for firms with 500 lawyers or more.

To help close this “protection gap,” the Association of Corporate Counsel recently published “Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information”, or the ACC Model. This document, which specifies baseline security measures and best practices legal departments may expect from outside counsel, is intended to serve as a benchmark guide for law firm information security practices. Because it offers an information security model containing key security capability protocols, law firms should seriously consider requiring that their vendors follow these same model controls.
The ACC Model offers 13 key practice areas or recommended controls and guidelines on which law firms should focus. These include the following:

1. **Policies and Procedures.** The ACC Model says Outside Counsel should have the appropriate technical and organizational measures to protect Company Confidential Information (CCI). Additionally, internal policies governing the protection of sensitive information should be in place. Sufficient resources must also be available to effectively pursue all measures and policies in place, and to ensure continuing maintenance of information security standards.

2. **Retention and Return/Destruction.** In order to most effectively safeguard data, Outside Counsel must retain CCI for as long as necessary to support clients. Such information must then be returned, deleted or destroyed unless it falls under an exception (such as daily email exchange). Firms should also be prepared to certify these steps have been taken within 30 days of any request.

3. **Data Handling.** The ACC Model establishes guidelines for data encryption, whether in storage, rest or in transit. Data breach notifications and compliance with relevant laws are also covered.

4. **Physical Security.** Cybersecurity is just one component of effective information security. The ACC Model instructs Outside Counsel to provide physical protection against outside incursions at storage centers or data processing facilities, and offers guidance on how to maintain appropriate physical security.

5. **Logical Access Controls.** The ACC Model instructs Outside Counsel to institute access controls that restrict CCI based on a principle-of-least-privilege model, which restricts access to system information or resources to only those necessary for a user to perform his or her job. This control also includes security measures such as two-factor authentication (requires username and password plus another layer of validation), complex and frequently changing passwords and the inability of users or developers to modify code, systems configurations or database environments.

6. **Monitoring.** Outside counsel should continually monitor its networks, employees, contract workers, and subcontractors for evidence of malicious activity or any behavior that could compromise the Company Confidential Information. This monitoring must remain in accordance with all relevant laws.

7. **Vulnerability Controls and Risk Assessments.** The ACC Model calls for annual vulnerability tests and assessments (including penetration testing and code reviews) on all systems that hold sensitive data.

8. **System Administration and Network Security.** It’s critical for Outside Counsel to maintain strong safeguards against external threats. Because of this, Outside Counsel should ensure the use of up-to-date anti-virus applications, firewalls, intrusion detection and prevention measures and other standard network security features.

“Given the critical nature of protecting their clients’ sensitive data, many law firms would benefit from a comprehensive information security program designed to meet modern security threats, whether internal, external or from a third party vendor.”

9. **Security Review Rights.** Outside Counsel should agree to allow periodic security procedure reviews as formally requested and negotiated.

10. **Industry Certification/Additional Security Requirements.** Outside counsel may agree to become ISO 27001 certified and implement any additional security steps requested by the hiring company.

11. **Background Screening of Outside Counsel Employees, Subcontractors, and Contingent Workers.** The ACC Model instructs outside counsel to screen all employees, contractors and contingent workers with access to CCI. The Law Firm must then annually certify that all workers have passed this screening.

12. **Cyber Liability Insurance.** Outside Counsel should maintain at least $10 million in cyber liability insurance from an insurer with a minimum A-minus rating from Standard and Poors or equivalent agency.

13. **Subcontractors.** Outside Counsel is responsible for all subcontractors used by Outside Counsel. All subcontractors who have access to CCI must follow the applicable security protocols within the ACC Model.

By adopting the ACC Model, Outside Counsel can help ensure that all confidential data remains well-protected, and that relationships with clients remain strong.

continued on page 4
AREAS OF FOCUS
Because the model is so comprehensive, law firms are advised to focus on a few key areas when beginning the implementation process.

First, firms should focus on the business aspect. This involves determining what data is sensitive and how to present security environments to customers.

Second, law firms should turn their attention to people—determining which staff members are best-suited to the critical task of ensuring security policies are followed.

Next, the process should be considered. Law firms should evaluate how to create processes that best serve security objectives. One example: The creation of a Computer Security Incident Response Team to quickly address and contain potential threats.

Finally, law firms should consider intrusion. This includes automated network protection applications and other technical solutions.

By focusing on these four key areas, law firms can set the conditions for smooth ACC Model implementation.

UNDERSTANDING SUPPORTING COMPLEMENTARY SECURITY MODELS
It should also be noted that the European Union takes a more vigorous approach to information security, viewing it as a fundamental right of its citizens. This posture was recently codified by the adoption of the General Data Protection Regulation (GDPR), a European Union edict that will create stringent data privacy restrictions after going into effect on May 25, 2018, impacting data processing within the EU or when data is transferred out of the EU. Violations of this regulation opens organizations up to penalties that may run into the tens of millions, so law firms should be aware of how information security requirements vary by jurisdiction.

CYBERSECURITY REQUIREMENTS FOR NEW YORK STATE
New York State has put in place a cybersecurity regulation known as NYCRR 500 Part 23 addressing cybersecurity of financial institutions, which went into effect March 1, 2017.

Also known as “Cybersecurity Requirements for Financial Services Companies”, the rules require banks, insurers, and other “covered entities” to meet minimum cybersecurity standards.

The regulation limits covered entities to those operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] Banking Law, the Insurance Law or the Financial Services Law. The regulation also exempts small organizations (less than 10 employees in NY or $5mil in revenue from NY business operations). Covered entities must provide annual certification of compliance, starting February 15, 2018.

The new regulation also outlines specific security measures for any third-party service provider that maintains, processes, or otherwise electronically accesses nonpublic information through its provision of services to the covered entities. Covered entities will need to have written policies and processes regarding third parties, and perform due diligence in evaluating third parties’ cybersecurity capabilities and ensuring minimum security measures are met, along with performing periodic assessments.

CONCLUSION
A commitment to key information security principles, such as those in the ACC Security Model and other frameworks like the GDPR and NYCRR, offers a variety of critical benefits. These possible benefits include the safeguarding of sensitive customer and company data; the generation of additional business (particularly with firms with clients in highly-regulated areas such as finance); lowered liability and assured compliance with company-required security policies.

Given these advantages—and the increasing challenges of today’s security landscape—law firms seeking to improve their information security practices should give strong consideration to adopting the ACC Model.

LEARN MORE
To learn more about how CT can help you better manage your compliance requirements, contact your CT representative or call 855.316.8948 (toll-free U.S.)