GC Requires Outside Law Firms to Encrypt Communications

The general counsel of Marsh & McLennan Companies has started requiring the company's biggest outside law firms to use an anti-hacking electronic communication technology known as Transport Layer Security, according to a report from **Bloomberg Law**.

The report quotes Peter Beshar: "What we have done here is gone out to 12 or so of the biggest law firms on the most sensitive matters and insisted, 'You can't communicate with us other than through TLS,' and everyone has signed up by it."

Beshar identified three of the firms are Cravath, Swaine & Moore, Davis Polk & Wardwell and Gibson Dunn & Crutcher.

TLS prevents any unauthorized senders or recipients from entering and intercepting communication – protecting "data in transit" from being hacked, explains reporter **Casey Sullivan**.

Read the Bloomberg article.

Join Our LinkedIn Group

D&O Insurance in a Time of Technological and Enforcement Uncertainty

Anderson Kill's 15th Annual D&O Conference, "**D&O Insurance in the Era of Technological and Enforcement Uncertainty**," will be presented Thursday, June 8, 2017, 3-5 p.m. EDT.

The event will be in the upper story of the D&D Building, 979 Third Ave., 14th Fl., New York 10022.

Directors and officers face an era of technological and enforcement uncertainty, the firm said in a news release.

Anderson Kill's annual D&O conference will feature a review of 2016 and a look ahead to 2017 for D&O liability and insurance. The conference also will feature a hypothetical D&O claim arbitration to explore key D&O insurance coverage issues in the context of a cyber claim, and will include a panel of policyholder attorneys, an arbitrator and an insurance company attorney.

Every organization faces data breach risk, whether through inadvertent data disclosure, computer system malfunction, or computer hacking. Data breaches cause real and severe peril.

The session will address the interplay of D&O insurance with other insurance policies in cyber claims, including crime insurance, property insurance, GL coverage, and cyber specialty insurance policies.

In addition, a panel of D&O insurance brokers will review major emerging D&O risks and provide a state of the market, highlighting key coverage terms to seek and avoid.

A cocktail reception follows the event (5:00-6:30 p.m.).

The D&O conference is complimentary for general counsel and risk managers: Use CODE AK005

Speakers:

William G. Passannante, Esq.
Shareholder
Anderson Kill
Conference Moderator

Joshua Gold, Esq.
Shareholder
Anderson Kill
Chair, AK's Cyberinsurance Group

Raymond A. Mascia, Jr., Esq.
Attorney
Anderson Kill

Vivian Costandy Michael, Esq.
Attorney
Anderson Kill

Jonathan E. Meer
Attorney at Law
Wilson Elser Moskowitz Edelman & Dicker LLP

Roger M. Moak
Arbitrator-Umpire-Mediator

R. Damian Brew
Managing Director, FINPRO
Marsh USA, Inc.

James McCue
U.S. Financial Institutions Practice Leader
Aon's Financial Services Group

Register for the event.

Join Our LinkedIn Group

Invitation: Summer Legal Conference, Berlin

Knowledge Nomads' **Summer Legal Conference** in Berlin July 23-29, 2017, will feature sessions on law in the age of hyperconnectivity, legal issues in the sharing economy, and the legal fallout from Volkswagen's emissions scandal.

The event will be at Berlin's Radisson Blu Hotel.

The CLE-qualified sessions will feature a diverse group of speakers, including a broad range of nationalities, backgrounds and ages.

Interspersed with the the presentations will be an arts and culture day with a choice of seven tailor-made tours, a trip to the home of Volkswagen, and a closing dinner on top of the German Federal Parliament Bundestag building.

Other side events will include guided tours, dinners, receptions, concerts, a gallery tour and more.

Register or get more information.

Are You Prepared for GDPR? Take the Survey

The General Data Protection Regulation (GDPR) will become law in all EU jurisdictions on May 25, 2018 and will impact organizations that handle EU citizen data for any number of reasons, from employment to customer relations to marketing. Just because a company is not based in or even operating in the EU doesn't mean GDPR won't apply.

It is a broad and wide-ranging regulation that is posing significant challenges for the types of clients Yerra serves, namely global corporations in highly-regulated industries such as banking, consumer goods and pharmaceuticals.

To gauge readiness for GDPR across industries and global regions, Yerra has launched an **industry survey** to help benchmark where global corporations are in their preparations. The GDPR Reality Check survey is being run in collaboration with the Blickstein Group and will be open for submissions through the end of May 2017.

Take the survey.

Join Our LinkedIn Group

Law Firm Sues Insurer Over $700K in Lost Billings Due to Ransomware Attack

A small Rhode Island law firm has filed a lawsuit against its insurance company after the insurer refused to pay $700,000 in lost billings following a ransomware attack on the firm that locked down the firm's computer files for three months, reports CloudNine's **eDiscovery Daily Blog**.

Doug Austin's report, based on a story in the ***Providence Journal***, explains that Moses Afonso Ryan Ltd. is suing its insurer, Sentinel Insurance Co., for breach of contract and bad faith. The insurer denied the plaintiff's claim for lost billings over a three-month period when the documents were frozen by a hacker's ransomware attack. The hacker encrypted the law firm's computer files, offering to unlock them if a ransom were paid.

The suit says the infection disabled the firm's computer network, meaning lawyers and staffers "were rendered essentially unproductive."

Read the eDiscovery Daily Blog article.

Join Our LinkedIn Group

Hackers Face $8.9 Million Fine for Law Firm Breaches

Three Chinese stock traders were ordered to pay $8.9 million in fines and penalties for hacking into two law firms and stealing information on upcoming mergers and acquisitions and then leveraging the information to trade stocks, according to a **Dark Reading report**.

A federal court in New York found that the three hackers installed malware on the law firms' computer networks, enabling them to view emails on mergers and acquisitions in which the firms were involved. Then they used that information to buy stock in at least three public companies prior to their merger announcements, according to the Securities and Exchange Commission.

The firms aren't identified in the complaints, but **Law360 reports** they appear to be Weil Gotshal & Manges and Cravath Swaine & Moore, based on information in charging documents.

Read the Dark Reading article.

Join Our LinkedIn Group

On-Demand: Before You Outsource, Protect Your IP & Mitigate Open Source Risks

Black Duck Software has posted a complimentary on-demand webinar discussing ways organizations can outsource to meet their development needs and also address open source security and management risks before giving contractors access to their valuable technologies.

"Today's rapidly changing technologies, including the proliferation of open source and the accelerating shift to the cloud, are increasing the use of outside experts for both application development and IT solutions," the company says on its website. "At the same time, IP security is top of mind worldwide."

The presenter is Jim Markwith, co-founder and managing partner of Symons Markwith LLP's Seattle and Washington, DC area offices.

He is an experienced technology and corporate transactions attorney with over 20 years of experience. His clients range from start-ups to fortune 50 technology leaders, including computer software, on-line retail, and Healthcare IT product and service developers.

Prior to private practice, Markwith held executive and senior in-house legal positions with Microsoft, Adobe Systems, and Allscripts Healthcare. He received his J.D. degree from Santa Clara University School of Law, and is a member of the California, Washington, DC, and Washington State Bar Associations.

[Watch the on-demand webinar](#).

Connected Product Intensive: Regulatory Compliance and Risk Management Roundtable

Keller and Heckman will produce a new seminar, "**The Connected Product Intensive: A Framework for Regulatory Compliance and Risk Management**," May 2-3, 2017 in San Francisco, CA.

Keller and Heckman's Connected Products Team will focus on the regulatory and litigation risks affecting connected products, and offer practical tips on compliance, risk avoidance, and risk management. Learn how to keep your customers safe and secure and to protect your company's reputation and investments.

Highlights from the agenda include:

- Guidance on developing compliance frameworks
- Drafting privacy policies
- Responding to a security breach and best practices for encryption
- Environmental considerations including California's

Proposition 65 and state green chemistry laws
- FCC issues from equipment certifications through spectrum availability
- Handling product recalls, crisis management, and product liability litigation
- Energy efficiency considerations
- Advertising and marketing emphasizing claims, price, safety, and social media
- Rules surrounding In-app purchases
- End-User License Agreements

Register for the seminar.

The Case for Continuous Open Source Management

Speakers from Black Duck Software and Wolters Kluwer will be presenters in a **webinar** addressing key open source security and management questions.

The complimentary event will be Wednesday, March 22, at 11 a.m. Eastern time.

Speakers will be Bob Genshaft, Director Strategic Programs at Wolters Kluwer, and Black Duck's VP and General Manager On-Demand Audits Phil Odence.

“Companies are constantly seeking ways to ensure their application code is secure and effectively managed. For example, M&A acquirers conduct one-time code audits on companies they are buying to avoid legal, operational or security pitfalls. Other organizations are proactive, using an an ongoing solution to make sure their application code is secure and well managed on a day-to-day basis. Increasingly, many companies are opting to use both approaches,” Black Duck says in a release.

Topics will include:

- When is it appropriate to conduct an audit?
- When should your company consider an ongoing solution?
- What are the benefits of doing both?

Register for the webinar.

Is Your Board Prepared to Oversee Cyber Risk?

The National Association of Corporate Directors has published the 2017 edition of the ***NACD Director’s Handbook on Cyber-Risk Oversight*** and made it available for free downloading.

The book is constructed around five core principles designed to enhance the cyber literacy and cyber-risk oversight

capabilities of directors of organizations of all sizes and in all industries, according to NACD.

This handbook provides

- foundational principles for board-level cyber-risk oversight;
- insight into management of cyber-risk oversight responsibilities; and
- tools to improve and enhance boardroom practices.

Download the handbook.

Five Tips for Addressing Information Security in Service Contracts

Data security must extend beyond the scope of a company's own office or network and to any of the company's service providers that have access to its data, warns Armand J. (A.J.) Zottola in Venable LLP's Digital Rights Review.

"A company can be held responsible for a data breach involving its own data, regardless of whether the company is directly responsible for managing its own data," Zottola writes. "The risks associated with sharing data with a service provider are best managed through the utilization of contract provisions

governing information security."

In his article, he offers guidelines to consider throughout the process of drafting information security provisions to govern the management, handling, and control of a company's data.

Headings for those guidelines include: research applicable legal requirements, set and meet minimum security standards through the establishment of an information security program, ensure the service provider isn't misusing data, determine security breach response procedures, and create audit requirements.

Read the article.

Join Our LinkedIn Group

Data Breach Trends and Tips: What State and Local Government Lawyers Need to Know

Practical Law's Mel Gates and Zach Ratzman on Thursday, January 12, 2017, at 1:00 p.m. Eastern will present a free, **75-minute webinar** that will explain recent data breach trends affecting state and local governments and provide tips on how to prepare for and help prevent a data breach or other cyber event . .

. before it happens.

Topics will include:

- Why state and local governments should be thinking about data breaches and other cyber events.
- Federal and state laws concerning personal information, data security, and breach notification.
- What reasonable security measures are and how they can impact a government entity's regulatory and litigation exposure.
- The basics on today's cyber threats with recent case studies of data breaches that have affected state and local governments.
- Recommendations on how government lawyers can play a key role in protecting their organizations.

A short Q&A will follow.

Presenters:

Mel Gates, Senior Legal Editor, Privacy & Data Security, Practical Law
Melodi (Mel) Gates, CIPP/US joined Practical Law from Squire Patton Boggs (US) LLP, where she was a senior associate focusing on cybersecurity and privacy issues, including in the health information technology field. Prior to practicing law, Mel worked for over twenty years in the telecommunications industry, last serving as chief information security officer (CISO) for a large network provider. She is also an appointed member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee (DPIAC).

Zach Ratzman, Director of Public Sector, Practical Law
Zach Ratzman joined Practical Law from the U.S. Department of Homeland Security's Office of the General Counsel in Washington, DC, where he advised senior DHS leadership on privacy, information sharing, and congressional oversight matters. Before that, Zach worked for nearly a decade at

several major New York City law firms, where his practice focused on securities and accounting fraud litigation. Before entering private practice, he clerked for the late Honorable Harold Baer, Jr. in the Southern District of New York. Zach is the Director of Practical Law's Public Sector Service.

Register for the webinar.

New Research Reveals: Phishers Launch a New Attack Every 30 Seconds

RSA has witnessed a huge uptick in targeted phishing email attacks in recent months, the company **reports on its website**.

"In Q2 alone, RSA identified more than 515,000 phishing attacks in the global market – a 115% rise over Q1 2016 and a remarkable 308% increase over the same time period last year," writes **Heidi Bleau**. "The U.S. continued to be the most attacked country, with 48% of global phishing volume, as well as the top hosting country, hosting 60% of all global phishing attacks. The total cost to global organizations from phishing: $9.1 billion."

RSA describes a new fraud tutorial, called “Jungle Money,” found in an underground forum. The tutorial tells fraudsters how to create a network of private e-Wallet accounts that are converted through online store merchant services and funneled into a business class e-Wallet account. Following the instructions, a scammer can be protected from discovery by making it difficult to tie the different accounts to one another.

“The scheme includes creating a number of shell accounts via Virtual Credit Cards (VCC), as well as multiple shell e-Wallet accounts, and using them to ‘juggle’ funds between the accounts by charging one account against another for a purchase or service. They then quickly request a chargeback from one of the accounts, thereby receiving a full refund and quickly cashing out the funds,” according to the report.

Read the article and download the report.

China Stole Data From Major U.S. Law Firms

A series of security breaches that stuck prestigious law firms last year was more pervasive than reported and was carried out by people with ties to the Chinese government, according to evidence reported by ***Fortune***.

In the cases studied by the magazine, hackers broke into BigLaw firm partners' email accounts and passed messages from their victims' in-boxes to outside servers.

"The evidence obtained by Fortune did not disclose a clear motive for the attack but did show the names of law firm partners targeted by the hackers," writes reporter **Jeff John Roberts**. "The practice areas of those partners include mergers and acquisitions and intellectual property, suggesting the goal of the email theft may indeed have been economic in nature."

Read the *Fortune* article.

New e-Posting Regulations, Featuring Locke Lord LLP – Webcast

eSignLive by VASCO and **Insurance Networking News** will present a **complimentary webinar** on how updated regulatory laws are allowing companies to improve the process of buying insurance for consumers, while ensuring security, compliance and enforceability, on Dec. 13, beginning at 2 p.m. Eastern time.

Intended to improve the process of buying insurance for consumers, there have been recent updates to laws that allow insurance companies to post policies, forms, and endorsements

on a website rather than printing these documents on paper.

As you look to take advantage of this new regulatory environment, questions related to how this can be done in a compliant way will arise.

Webcast highlights:

- E-Posting and E-Delivery defined
- Update from PCIAA on the progress of legislative adoption of e-posting laws
- The intersection between ESIGN, UETA and state insurance laws on e-signatures and records
- How to demonstrate insured consent to do business electronically
- Best practices for ensuring security, compliance and enforceability
- A live demonstration of insurance policy electronic posting

Register for the webinar.

Cybersecurity Attorney, Former Texas Chief Information Security Officer

Joins Gardere

Information security expert **Edward H. Block** has joined **Gardere Wynne Sewell LLP** as a senior attorney in its Austin office. Block joins the firm from the Texas Department of Information Resources, where he served as the chief information security officer (CISO) and the cybersecurity coordinator for the state of Texas.

With more than 20 years of experience in the cybersecurity arena, Block primarily focuses on the effects of emerging law on personal privacy at the state, federal and international levels. He has assisted and managed technical teams performing all aspects of information security work, and has developed information security policies, standards and guidelines that balance protection of information assets with legal and functional requirements.

In a news release, the firm said Block joins Gardere's litigation practice and is a member of the firm's internet, eCommerce and technology team, as well as its cybersecurity and privacy legal services team. Block will work closely with the firm's government affairs team on cybersecurity law and regulation, as well as collaborate with the corporate practice group to evaluate parties' security postures, policies and procedures in mergers and acquisitions to ensure an integrated approach to addressing security risk during the transition. In addition, Block will assist clients with establishing security, breach and disaster recovery polices and will counsel on cyber insurance issues, including evaluating policy compliance.

"Eddie's unique background in information security will be an enormous asset to our clients in navigating their evolving cybersecurity needs and challenges," says Kimberly A. Yelkin,

executive partner in Gardere's Austin office and chair of the government affairs team. "We are thrilled to welcome Eddie to the team."

Prior to his time at the Texas Department of Information Resources, Block was a senior product security engineer at Polycom Inc. and was the information security officer for the Employees Retirement System of Texas. He is a Certified Information Systems Security Professional (CISSP), Certified Information Privacy Manager (CIPM), Certified Information Systems Auditor (CISA) and a Certified Ethical Hacker (CEH). Block earned his undergraduate degree at Loyola Marymount University and his juris doctorate at St. Mary's University School of Law.

NY AG Warns Law Firms About Phishing Scam

New York's Attorney General Eric Schneiderman issued a warning on Wednesday about a phishing scam in which hackers pose as representatives from from his office and target attorneys, according to a **Bloomberg Law report**.

Schneiderman's **press release** quotes a phony email in which the hackers suggest a complaint has been filed against the recipient's law firm.

"The goal of such emails is to trigger the recipient to click a link or open an attachment through which the hacker can gain access to the server, and any sensitive information on your computer such as credit card data and social security

numbers," the report says.

[Read the Bloomberg article](#).

FinCEN Issues Guidance on Cybersecurity

By Patty P. Tehrani
Lawyer and Founder of Policy Patty Toolkit

The cybersecurity regulations keep coming. Following New York's proposed regulation on cybersecurity, and notice from banking regulators on proposed cybersecurity rules, the Financial Crimes Enforcement Network (FinCEN) has issued an advisory and related FAQ.

The advisory includes key definitions relevant to cyber-related incidents as follows:

• Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

• Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

• Cyber-Related Information: Information that describes

technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

The advisory explains how BSA requirements apply to cyber-events, cyber-enabled crime, and cyber-related information with guidance on:

- reporting cyber-enabled crime and cyber-events through SARs;
  - consider all available information surrounding the cyber-event, including its nature and the information and systems targeted;
  - determine monetary amounts involved in the transactions or attempted transactions (should consider in aggregate the funds and assets involved);
  - know other cyber-related SAR filing obligations required by their functional regulator;
- including relevant and available cyber-related information (examples provided – IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information) in SARs to:
  - provide complete and accurate information, including relevant facts, to the extent available:
    - description and magnitude of the event;
    - known or suspected time, location, and characteristics or signatures of the event;
    - indicators of compromise;
    - relevant IP addresses and their timestamps;
    - device identifiers;
    - methodologies used; and
    - other information the institution believes is relevant;
  - refer to the FAQs for additional information on reporting cyber-related information in SARs;
- collaborating internally between BSA/Anti-Money Laundering (AML) units and other units to identify suspicious activity to:

o make sure to internally share relevant information from across the organization to help reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units;
o use cyber-related information to:
 help identify suspicious activity and criminal actors;
 develop a more comprehensive understanding of their BSA/AML risk exposure;
 use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime;
 provide for more comprehensive and complete SAR reporting;
• sharing information among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime to:
o identify threats, vulnerabilities, and criminals; and
o note the extension of Section 314(b) of the USA PATRIOT Act as a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements— to encourage information sharing.
The supplemental FAQs provide additional guidance on reporting obligations for cyber events and cover the following questions:
• What information should a financial institution include in SARs when reporting cyber-events and cyber-enabled crime?
• How should a financial institution complete SARs when reporting cyber-events and cyber-enabled crime
• How should cyber-events and cyber-enabled crime be characterized in SARs?
• How does a financial institution report numerous cyber events in SARs?
• Is a financial institution required to file SARs to report continuous scanning or probing of a financial institution's systems or network?
• Should a SAR be filed in instances where an otherwise reportable cyber-event is unsuccessful?
• Does FinCEN now require financial institutions' BSA/AML

units to have personnel/systems devoted to cybersecurity?
• Are BSA/AML personnel now required to be knowledgeable on cybersecurity and cyber-events?
• Can financial institutions use Section 314(b) of the USA PATRIOT Act to share cyber-event and cyber-enabled crime information with other financial institutions
Note: These new FAQs replace prior guidance provided by FinCEN.

FinCEN hopes the guidance will help reduce cyber risks for financial institutions as serve as a reminder on:
• their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime;
• how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime;
• compliance with BSA requirements or other regulatory obligations for financial institutions does not absolve them from having to comply with federal and state notice/reporting requirements and guidance on cyber-related incidents;
• encouraging collaboration:
o within financial institutions—between employees combating cyber-crime and employees combating money laundering;
o information sharing between financial institutions to again more effectively combat cyber-crime; and
• filing a Suspicious Activity Report (SAR) does not relieve it from any other applicable notice requirements of events impacting critical systems and information or of disruptions in their ability to operate.

Note: Under the Bank Secrecy Act, financial institutions must file SARs to report suspicious activity.

Thomson Reuters, Pillsbury, FireEye Align to Provide Cybersecurity Compliance Program

Spurred by the growing and often contradictory cybersecurity regulatory burden facing companies, Thomson Reuters, Pillsbury and FireEye have formed an industry-first collaboration to help corporations meet new regulations and manage risk related to cybersecurity. In a release, the companies said this alliance affords institutions expertise and resources from a holistic, multi-pronged approach to cybersecurity risk assessment and due diligence that combines legal counsel, technical assessments and legal managed services to help meet a variety of internal, external and regulatory standards.

The release continues:

As targeted attacks become more sophisticated, complex and commonplace, organizations cannot rely on the patchwork of industry standards to use as a base for their cybersecurity or risk management program. Each organization should determine its own risk and address any issues or concerns before a problem arises. However, even a casual review of the news shows that many organizations are not meeting this seemingly minimal obligation with widespread success.

The alliance between Thomson Reuters, Pillsbury and FireEye provides the resources and guidance organizations can rely upon to help manage cyberrisk, especially as additional regulations in this area expand and evolve. Pillsbury, a leading international law firm, will help companies navigate

the myriad regulations, standards and guidelines they face as well as provide them with legal counsel related to compliance and risk management. The Thomson Reuters Legal Managed Services team will leverage its experience and efficient processes to review contracts and agreements with third-party suppliers and assist in implementing key changes to such processes or agreements advised by Pillsbury. FireEye, an industry-leading cybersecurity company, will perform the technical risk assessments, advanced testing and response readiness to help each organization's defense posture match the threats to their specific industry and operations.

"Cyberthreats and the regulations created to counter have grown incredibly complex," said Brian Finch, partner and co-chairman of Pillsbury's privacy, data and cybersecurity practice. "With that in mind, it is essential to bring multiple perspectives and skill sets together in order to attack the problem. The recently released cybersecurity regulations from the New York State Department of Financial Services cemented our belief that no one organization can fully assist a company in protecting itself from criminal attack and regulatory obligations. The opportunity to work with industry leaders like FireEye and Thomson Reuters to help companies solve those multiple objectives is a truly exciting one."

Rich Stegina, vice president of Strategic Partnerships at FireEye, commented, "FireEye provides our clients with a global team of experts that can assess an organization's cybersecurity situation via a range of pre-breach service offerings specific to the needs and goals of that organization. By strategically partnering with leaders in the legal industry – Pillsbury and Thomson Reuters – we can address the complex cyberthreats that the market and specific organizations are facing."

Christy Weisner, director of Thomson Reuters Legal Managed Services, noted that a key element to this offering, and any

cybersecurity risk assessment program, is the analysis of third-party agreements for gaps and degree of risk. “Our Legal Managed Services group at Thomson Reuters already supports clients across all sectors with ongoing contract lifecycle management and compliance solutions, and this alliance ensures clients receive a comprehensive team to address cyberrisk. Our managed services experts will evaluate each contract that involves client data or information systems and, following Pillsbury’s guidance, assist in renegotiation and redocumentation if needed.”

The Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency are considering applying enhanced standards to address this issue for a sensitive and critical area of the U.S. marketplace. Additionally, the New York State Department of Financial Services recently issued regulations in “Cybersecurity Requirements for Financial Services Companies.” Covered entities must adhere to a wide range of cybersecurity requirements, including the establishment of a cybersecurity program and ensuring that third-party service providers are holding information in a secure manner.

Five Questions GC Should Ask

About Privacy and Cybersecurity in Third-Party Contracts

While a company cannot eliminate risks involving compromised data and systems, there are some actions that a company should take to protect data in the hands of third-party suppliers, advises **Mayer Brown LLP**.

In **an article** posted on the firm's website, authors Rebecca S. Eisner, Lei Shen and Lindsay T. Brown discuss five privacy- and security-related questions that a general counsel should ask regarding company data in the hands of third-party suppliers and other business partners.

They questions they discuss at length are: Have We Assessed Our Security and Privacy Risks? How Robust Is Our Oversight of Third Parties Who Have Our Data or Access to Our Networks? Do We Have Appropriate Contractual Protections? How Do We Monitor Developments? and Do We Address Privacy and Security in Other Transactions, Such as M&A?

Read the article.