Panel Discussion
Hot Topics In Cybersecurity

Panelists:

Luke Dembosky
Debevoise & Plimpton

John Thomas (JT) A. Malatesta II
Maynard Cooper Gale

Andrew P. Obuchowski Jr.
RSM US LLP

Rusty Yeager
HealthSouth Corporation

Moderator:

India E. Vincent
Burr & Forman

Items to Assess in a CyberSecurity-Readiness Audit

1. Data Use and Backup Mapping
2. System Diagrams and Logs
3. Network Security Assessments - internal and external
4. Employee Education - frequency, substance and attendance
5. Penetration Testing - frequency, scope, results
6. Insurance -scope of coverage
7. Contract Review - balancing of cyber-risks in contracts
8. Legal Landscape Relevant to Industry
9. Vendors to Assist in the Event of an Incident - contacts and contracts
10. Law Enforcement Contacts
11. Planned Redundancy for System Recovery

Consider a readiness audit as a starting point for cybersecurity efforts and on a regular, periodic basis going forward to assess strengths and weaknesses in the plans and procedures.

Developing a Data Security Policy

1. Consider results of any risk assessments that have been performed and address any weaknesses in the policy.
2. Have a complete understanding of your network architecture and storage of all of your data. Update all data storage and network mapping as needed.
3. Understand which portions of data stored in the system are the most valuable and why. Prioritize efforts accordingly.
4. Determine which data in the system, if any, should be encrypted.
5. Consider the likely entry points into the network and develop appropriate security strategies to limit unauthorized entry at these points.
6. Consider any supply chain risks. Audit suppliers if necessary.
7. Develop a comprehensive mobile device policy.
8. Mitigate liability through contractual relationships with clients, customers, vendors, etc.
9. Research and understand likely threats in your industry and for your business.
10. Document reporting requirements that may apply to the organization in the event of a breach.
11. Audit and test security measures.
12. Create and practice response plans.
13. Understand the government's ability to assist with cybersecurity

Developing an Incident Response Plan

1. Identify the key internal employees required for team and contact information for each team member
    a. Determine who will lead the team and each team members' responsibilities
    b. Needs to include C-Suite
    c. Determine who is authorized to activate the plan and under what conditions the plan will be activated

2. Identify external consultants that must be part of the response team and list their contact information. Negotiate contracts in advance to be activated when needed.
    a. Forensic Consultant
    b. Legal Counsel with cyber incident response experience
    c. Public Relations Consultant/Firm
    d. Incident Response Consultant
    e. Others that may be specific to your industry or needed based on gaps in your internal team

3. Prepare the Response Plan in binders and include a laminated call list
    a. Each team member should have a binder and a laminated call list

4. Communication Strategy
    a. Assume that you will need to communicate outside of the compromised system for some period of time.
    b. Rely on legal counsel to guide you in maintaining privileged nature of conversations

5. Technical Response: Assess; Secure; and Preserve

6. Legal Response and Notifications

The Incident Response Plan should be practiced regularly in table topic settings and, if possible, in Red Team scenarios.

CyberSecurity Terms

What is CyberSecurity?

CyberSecurity	-	Strategy, policy, standards and procedures for protecting information assets by identifying and responding to threats to information that is processed, stored or transported electronically.
Attack	-	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. The intentional act of attempting to bypass one or more security services or controls of an information system.
Bring Your Own Device (BYOD)	-	The use of personally owned mobile devices such as smartphones or tablets in the workplace.
Chief Information Security Officer (CISO)	-	The person in charge of information security within the enterprise.
Chief Security Officer (CSO)	-	The person usually responsible for all security matters both physical and digital in an enterprise.
Data Breach	-	An unauthorized access, movement, or disclosure of sensitive information by an actor or to a recipient who does not have authority to access the information. Sometimes referred to as a "data spill".
Disaster Recovery Plan (DRP)	-	A set of human, physical, technical and procedural resources that allow the recovery of an IT system in the event of a disruption or disaster.
Disruption	-	An event causing unplanned interruptions in operations of IT systems.
Event	-	An observable occurrence in an information system or network, which may provide an indication that the occurrence is actually an Incident.
Hacker	-	Anyone who attempts to or gains access to an information system without authorization. Frequently used for individuals violating security policies to access systems for malicious reasons or personal gain.
Incident	-	An adverse Event that results in or could result in adverse consequences to an information system or the information stored on the system, and it may require a Response to mitigate the consequences.
Intrusion	-	An unauthorized act of bypassing the security mechanisms of a network or information system.
Threat	-	Something that could cause harm to a system or organization. A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence.

Types of Threats:

Advanced Persistent Threat (APT)	-	A threat from a sophisticated adversary with control over sufficient resources to allow the adversary to create multiple attack vectors (cyber, physical and deception) simultaneously, where the adversary pursues the objective repeatedly or continuously over an extended period of time, adapting to a defender's efforts to block the attack and maintains the level of interaction with the system needed to execute its objectives.
Backdoor	-	A tool installed by an attacker during or after an attack to give the attacker easier access to the compromised system in the future, by passing any security mechanisms that are in place. A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
Brute Force Attack	-	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found.
Bot	-	Malicious logic surreptitiously introduced into a computer or a network where the logic is under the control of a remote administrator. A larger collection of compromised computers known as a botnet. Synonym: zombie
Denial of Service	-	An attack that prevents or impairs the authorized use of system resources or services by flooding the system with so many requests it becomes overwhelmed and may stop operating altogether or operate at a significantly reduced speed.
Dictionary Attack	-	An attack that tries all of the phrases or words in a dictionary (or in a predefined list), to crack a password or key.
Distributed Denial of Service	-	A denial of service technique that uses numerous systems to perform the attack simultaneously.
Exfiltration	-	The unauthorized transfer of data out of a system.
Exploit	-	A technique to breach the security of a system or network in violation of security policy.
Honey pot	-	Programs simulating a network service (or services) designated on your computer's ports. The attacker assumes the system is running vulnerable services that can be used to break into the machine, and instead it allows you to log access attempts to those ports including the attacker's keystrokes. The information can help provide advanced warning of a more concerted attack.
Insider Threat	-	One or more persons in an organization who pose a risk of violating security policies or of accessing information and exploiting the vulnerabilities of the system with the intent to cause harm.

Keylogger	-	Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly.
Malware	-	Software that compromises the operation of a system by performing an unauthorized function or process that is most often used to cause damage to or obtain information a computer system without the owner's consent. Common types include viruses, worms, Trojan horses, spyware and adware.
Outside Threat	-	A person or group of persons external to an organization who are not authorized to access its assets and pose a potential risk to the organization and its assets.
Passive Attack	-	An attack that attempts to learn from or make use of data in the system, but does not attempt to alter the system, its resources, its data, or its operations.
Phishing	-	A digital form of social engineering designed to deceive individuals into providing sensitive information. This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.
Spear Phishing	-	An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim
Spoofing	-	Faking the sending address of a transmission to gain unauthorized and possibly illegal entry into a secure system.
Spyware	-	Software that monitors a computer user’s actions (e.g., web sites visited) and reports these actions to a third party, without the informed consent of that machine’s owner or legitimate user.
Supply Chain Threat	-	A threat implemented by exploiting the systems of a target's supply chain vendors.
Threat actor	-	An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. Synonym: threat agent
Trojan horse	-	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Virus	-	A computer program, usually containing destructive code, that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.
Worm	-	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Preventative Efforts:

Acceptable Use Policy	-	A policy that establishes the ranges and scope of use that are approved for a system and to which all users must agree before gaining access to the system.
Access rights	-	The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy
Antispyware	-	A program for detecting, blocking or removing forms of spyware.
Antivirus Software	-	A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents.
Authorization	-	A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. The process or act of granting access privileges or the access privileges as granted.
Behavior Monitoring	-	Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.
Biometrics	-	Physical characteristics such as thumb prints or hand prints used to determine authorized access.
Blue Team	-	A group that defends an enterprise's information systems against the Red Team (attackers) in a mock attack.
Business Continuity Plan (BCP)	-	A Business Continuity Plan is a written plan that documents the expected emergency response, backup operations, and post-disaster recovery steps that have been selected to help ensure the availability of critical resources in an emergency situation.
Computer Emergency Response Team (CERT)	-	A group of people with clear lines of reporting and responsibilities who act as a single point of contact for all incidents and issues related to information systems and who remain on stand-by to provide support in case of an information systems emergency.
Cyber Exercise or Operational Exercise or Tabletop Exercise	-	A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. These tests should be designed to ensure the adequacy of an incident response plan, a business continuity plan and a disaster recovery plan as well as the common understanding of all team members.
Disaster Recovery Site	-	Hot site. Fully redundant hardware and software, with telecommunications, telephone and utility connectivity to continue all primary site operations within minutes or hours following a disaster. The system includes frequent (often daily) synchronization of data) The most expensive disaster recovery option. Warm site. Partially redundant hardware and software, with telecommunications, telephone and utility connectivity to continue some, but not all primary site operations, to continue all covered

		operations within hours or days following the disaster. Synchronization of data usually happens daily or weekly. Offsite data backup tapes must be obtained and delivered to the warm site to restore operations. Cold site. Hardware is ordered, shipped and installed, and software is loaded. Basic telecommunications, telephone and utility connectivity exist but may need to be turned on to continue some, but not all primary site operations. After a disaster, relocation takes weeks or longer, depending on hardware arrival time. There is no synchronization of data between the sites, and significant data loss could occur. Offsite data backup tapes must be obtained and delivered to the cold site to restore operations. A cold site is the least expensive option.
Firewall	-	A hardware or software device that has the capability to limit network traffic between networks and/or information systems according to a set of predetermined rules.
Information Security Policy	-	An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
Intrusion Detection System (IDS)	-	Program or device used to detect that an attacker is attempting or has attempted unauthorized access to computer resources.
Intrusion Prevention System (IPS)	-	Intrusion detection system that also blocks unauthorized access when detected.
Patch	-	Fixes to software programming errors and vulnerabilities.
Patch Management	-	Acquiring, testing and installing multiple patches (code changes) to software or a computer system in order to maintain up-to-date software and often to address security risk.
Penetration Testing / Pen Test	-	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Red Team	-	An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.
Risk Assessments	-	Collecting information and assigning values to identified risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
Security Policy	-	An established rule or set of rules that govern the acceptable use of an organization's information and services to maintain an acceptable risk level and to protect the organization's information assets.
Supply Chain Risk Management	-	The process of identifying, analyzing, and assessing risk introduced by the information systems of a target's supply chain risk.
Threat Analysis	-	Evaluation of the characteristics of individual threats.
Threat Assessment	-	Identifying or evaluating entities, actions, or occurrences, that have or indicate the potential to cause harm.

Two-Factor Authentication	-	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.
White Team	-	A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Incident Response:

Attack Pattern	-	Similar cyber events or behaviors that may indicate a particular type of attack has occurred or is occurring.
Attack Signature	-	A characteristic or distinctive pattern of an attack that can be identified and used to match one attack to others.
Digital Forensics / Forensics	-	Specialized techniques for collecting, processing, preserving, retaining, analyzing, and presenting gathering, retaining, and analyzing system-related digital evidence for investigative purposes.
Incident Management	-	Management and coordination of activities associated with an Event.
Incident Response or Response	-	Activities addressing short term, direct effects of an Incident which may also help support short term Recovery efforts.
Incident Response Plan	-	A set of predetermined, documented procedures to detect and respond to a cyber incident.
Recovery	-	The activities occurring after an Incident or Event that are necessary to restore essential business services and operations.
Situational Awareness	-	Knowledge that the incident response team seeks that includes understanding the current and developing security posture and risks associated with a system and the current risk assessment, based on information gathered, observation and analysis, and knowledge or experience.

A Few Technical Terms:

Air-Gap	-	Physical separation or isolation of a portion of the system from other parts of the system or network.
Cloud Computing	-	A shared pool of resources available for provisioning and release through an on-demand network with minimal management effort.
DMZ	-	A screened or firewalled segment of a network that sits between the organization's internal network and external networks, such as the Internet. The DMZ is used for servers that need to be accessed by less trusted users or that must be accessible by external users.
Gateway	-	A point in the network that allows entry into another network.
Payload	-	The critical section of data in a transmission. In malware, the payload is the section of the transmitted data that contains the harmful data or code.

Proxy Server	-	Server that acts as an intermediary between users and others servers, validating user requests.
Router	-	Device that directs messages within or between networks
Server	-	Computer that provides data or services to other computers over a network
Virtual Private Network (VPN)	-	Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.
Zero-Day-Exploit	-	A vulnerability in software that is exploited before the software vendor is aware of the vulnerability and there are no patches yet available to address the exploit. These often occur on the day that new versions of software are made available.

Ten Cybersecurity Tips for Small Businesses

STOP | THINK CONNECT™

Broadband and information technology are powerful tools for small businesses to reach new markets and increase sales and productivity. However, cybersecurity threats are real and businesses must implement the best tools and tactics to protect themselves, their customers, and their data. Visit ***www.fcc.gov/cyberplanner*** to create a free customized Cyber Security Planning guide for your small business and visit ***www.dhs.gov/stopthinkconnect*** to download resources on cyber security awareness for your business. Here are ten key cybersecurity tips to protect your small business:

1. Train employees in security principles. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. Protect information, computers, and networks from cyber attacks. Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. Provide firewall security for your Internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. Create a mobile device action plan. Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. Make backup copies of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6. Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

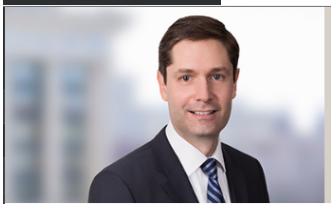
9. Limit employee access to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Passwords and authentication. Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

The FCC's Cybersecurity Hub at http://www.fcc.gov/cyberforsmallbiz has more information, including links to free and low-cost security tools. Create your free small business cyber security planning guide at www.fcc.gov/cyberplanner.

To learn more about the Stop.Think.Connect. Campaign, visit www.dhs.gov/stopthinkconnect.

Debevoise & Plimpton



Luke Dembosky
Partner
email | vCard

Washington, D.C.

Tel: +1 202 383 8020
M: +1 202 430 9923

Luke Dembosky is a litigation partner based in the firm's Washington, D.C. office and is a member of the Cybersecurity & Data Privacy practice and White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and emergency response, related civil litigation and regulatory defense, as well as national security issues.

Mr. Dembosky joined Debevoise in March 2016. Prior to joining the firm, he served as Deputy Assistant Attorney General for National Security in the National Security Division of the U.S. Department of Justice. In this capacity, Mr. Dembosky was the first to manage a new "National Asset Protection" portfolio covering all cybersecurity, economic espionage, export control and foreign investment review matters, giving him responsibility over a wide range of technology-related threats. In addition to working closely with the senior leadership of the Department of Justice, the Federal Bureau of Investigation and the National Security Council, Mr. Dembosky oversaw the division's Counterintelligence and Export Control Section and the National Security Cyber Specialists network of prosecutors throughout the United States. He also oversaw the Foreign Investment Review Staff and in that capacity regularly represented the Department of Justice and the Federal Bureau of Investigation in the Committee on Foreign Investment in the United States and in review of international telecommunications licensing matters.

From March 2013 to October 2014, he served as Deputy Chief for Litigation in the Computer Crime and Intellectual Property Section of the Department of Justice, where he supervised all cybersecurity and intellectual property crime prosecutions by the 35 attorneys in the section.

Mr. Dembosky was the senior official responsible for managing the Department of Justice's investigation and prosecution of numerous major hacking incidents, including

the cyber breaches of Sony Pictures, Target, Home Depot, Anthem and the Office of Personnel Management, among many others. He also managed the Department's cutting-edge operation to take down the GameOver Zeus botnet, for which he received the Attorney General's Award for Distinguished Service in 2015, and was involved in coordinating the takedown of the Silk Road online marketplace. Mr. Dembosky co-represented the Department in negotiations leading to a cyber accord with Russia in 2013 and the historic 5-point agreement signed by President Obama and President Xi Jinping of China in September 2015.

Before moving to the Computer Crime and Intellectual Property Section, Mr. Dembosky served as the Department of Justice's representative at the U.S. Embassy in Moscow. For two-and-a-half years, he managed the Department of Justice's transnational crime portfolio at the embassy, represented the United States in high-level diplomatic engagements with Russia and other countries, advised the Ambassador and other senior U.S. officials, and worked to build international cooperation on cyber, intellectual property and other matters. In 2012, he also co-represented the Department of Justice in cybersecurity negotiations in the United Nations Group of Government Experts.

From 2002 to 2010, he served as an Assistant U.S. Attorney for the Western District of Pennsylvania, where he prosecuted numerous large-scale, national and international cybersecurity and intellectual property crime cases. He also served in the Computer Hacking and Intellectual Property Unit and conducted investigations related to complex financial crimes and money laundering. For his prosecution of *U.S. v. Max Ray Butler*, also known as the "Iceman" case, Mr. Dembosky received multiple awards, including a superior performance award from the U.S. Secret Service. The case is the subject of the books *Kingpin* and *DarkMarket* and an episode of the television series American Greed. Mr. Dembosky was a litigation associate with two law firms from 1996 to 2002, and he served as a law clerk to the Hon. Richard L. Nygaard of the U.S. Court of Appeals for the Third Circuit from 1994 to 1995.

He is admitted to the bars of Pennsylvania and Delaware and to appear before the Western and Eastern Districts of Pennsylvania, District of Delaware and U.S. Court of Appeals for the Third Circuit.

Mr. Dembosky earned his J.D *cum laude* from the University of Pittsburgh School of Law in 1994, where he was elected to Order of the Coif, Order of the Barristers and was

Managing Editor of the *University of Pittsburgh Law Review*. He received his B.A., with High Distinction, from Pennsylvania State University in 1990.

Education

- University of Pittsburgh School of Law, 1994, J.D.
- Pennsylvania State University, 1990, B.A.

Bar Admissions

- Pennsylvania
- Delaware

Not Admitted in Washington, D.C. / Practice Supervised by Members of the Firm

MAYNARD
COOPER GALE

John Thomas A. Malatesta III

Shareholder | Birmingham
Phone: 205.254.1180
jmalatesta@maynardcooper.com
Fax: 205.254.1999

Practice Areas
Cybersecurity
Complex Litigation
Compliance and Investigations
General Litigation

Bar Admissions
State Bar: Alabama, New York
U.S. Court of Appeals: Eleventh Circuit
U.S. District Court: Alabama (Middle, Northern, Southern)

Education
University of Virginia School of Law (2004, J.D., Virginia Tax Review, Articles Editor; Virginia Sports and Entertainment Law Journal)
Washington and Lee University (2000, B.S., cum laude)

Biography

J.T. is the chair of Maynard Cooper's Cybersecurity practice. He also leads the firm's e-discovery practice.

Cybersecurity Risk Management and Data Breach Litigation

J.T. helps businesses develop cyber risk management and mitigation strategies, including the development and implementation of incident response plans, updating vendor management programs, and performing cybersecurity compliance audits.

J.T. is a NetDiligence® Breach Coach. He guides clients through the immediate and necessary steps following a data breach, including incident response, data breach notification, regulator inquiries and, if necessary, civil litigation. He has represented a number of clients in data breach litigation, particularly in the financial services and insurance industries.

J.T. is a frequent speaker on emerging issues in cybersecurity regulation and data breach litigation. He is one of a handful of lawyers from the across the country recently selected by the Sedona Conference to author an upcoming primer on data security. He is also members of Infragard, a public-private partnership between the FBI and the business community on cybersecurity, and the Sedona Conference Data Security and Privacy Liability Working Group.

Representative services include:

- Advising companies on cybersecurity oversight strategies for boards of directors and executive management
- Developing incident response plans
- Updating vendor and business partner contracts to ensure adequate privacy and data security safeguards are in place over non-public personally identifiable information
- Assisting companies with cybersecurity exams
- Conducting data breach investigations
- Examining domestic and international privacy laws
- Advising clients on customer and regulatory data breach notification obligations
- Evaluating existing policies, practices and procedures to determine if they comply with the controlling regulatory framework

MAYNARD
COOPER GALE

Attorney Bio (cont.)

- Counseling clients on cyber risk management and mitigation strategies
- Assessing available coverages and exclusions within cyber liability policies
- Evaluating the cybersecurity risk associated with mergers, acquisitions, and other business transactions
- Defending class action data breach lawsuits

Electronic Discovery and Data Management

J.T. has advised companies on electronic discovery from the day the Federal Rules of Civil Procedure were amended in 2006 to address the subject matter. He is a leading practitioner in the area, and has developed a reputation for cost-effectively managing the life cycle of electronically stored information (ESI) in complex litigation. J.T. helps client manage the entire spectrum of the Electronic Discovery Reference Model (EDRM) – Information Management, Preservation, Collection, Processing, Production and Presentation.

Representative services include:

- Advising companies on best practices for litigation holds
- Developing discovery protocols
- Drafting structured data discovery requests
- Negotiating discovery obligations
- Performing forensic investigations
- Developing cost-efficient document collection, analysis, review, and production strategies
- Representing corporate representatives in ESI Depositions
- Motion practice on electronic discovery obligations

J.T. also counsels companies on information governance initiatives that can be implemented in advance of litigation to proactively manage data, and reduce legal and financial risk. These include policies and procedures for record retention, e-mail management, computer usage, social media and Bring Your Own Device (BYOD).

General Litigation

J.T. began his law career as a litigator. For more than 10 years he has been a general litigator in the truest sense of the term. He has handled a variety of matters on behalf of OEMs, automotive suppliers, pipeline companies, municipal airports, manufacturers, financial services companies, broker dealers, construction companies, real estate investment trusts, insurance companies, movie retailers and individuals. He is listed by *Alabama Super Lawyers* in the area of Business Litigation. Representative cases that J.T. has handled can be found under Experience.

J.T. received his J.D. from the University of Virginia School of Law and holds a B.S. from Washington and Lee University.

MAYNARD
COOPER GALE

Attorney Bio (cont.)

Experience

- Represent commercial health insurer in antitrust MDL
- Represent interstate common carrier of petroleum products in $162 million breach of contract action
- Represent insurance companies in data breach and identity theft cases alleging that personally identifiable information (PII) has been compromised
- Represent broker-dealer in action to enjoin vendor from discontinuing operation of e-mail service
- Represent OEM in franchise dealership litigation
- Represent municipal airport in Open Records Act inquiries and litigation
- Represented REIT in the HealthSouth Corporation shareholder derivative action in which the Plaintiffs sought recovery of $2.6 billion loss sustained in corporate accounting scandal
- Represents transit bus manufacturer in litigation matters around the country
- Represents manufacturing suppliers in actions involving breach of contract and breach of warranty
- National counsel for glass installation company
- Represented interstate common carrier of petroleum products in toxic tort litigation brought by several landowners alleging property damage and mental anguish
- Represent broker-dealers in FINRA arbitrations and state court cases
- Represented closely held corporation in AAA arbitration involving claims of breach of contract
- Represented movie retailer in several cases throughout the Southeast alleging civil RICO claims

Awards

- *Alabama Super Lawyers*® - Business Litigation, 2015; Rising Star, Business Litigation, 2011-2014

Affiliations & Civic Involvement

Affiliations

- American Bar Association
- Alabama State Bar Association
- New York State Bar Association
- Birmingham Bar Association
- InfraGard
- ESI Roundtable (Birmingham and Tampa chapters)

Andrew P. Obuchowski Jr.

Practice Leader, Digital Forensics and Incident Response Services
Director, Security and Privacy Consulting
RSM US LLP
United States of America
andy.obuchowski@rsmus.com
+1 617 241 1219

Summary of experience

Andrew Obuchowski is the practice leader and supports global operations for cybercrime and data breach investigations, digital forensics and incident response services within the security and privacy consulting group. Andrew possesses more than 20 years of experience, including 12 years of law enforcement investigations, instruction at numerous police academies, and long-time memberships in several computer and financial crime task forces. He is also currently an adjunct professor of criminal justice at Anna Maria College in Massachusetts, where he developed and teaches graduate and undergraduate programs in information security, digital forensics and cybercrime investigations.

As an industry leader and expert in his field, his team provides services and solutions for clients in preparation of and in response to matters involving a wide range of information security and privacy assessments and investigations.

Professional experience

Prior to joining RSM, Andrew was a leader with Navigant's legal technology solutions group overseeing matters and developing business relationships, project plans, and policies/procedures surrounding data privacy and digital forensics. Andrew also managed teams responsible for data breach investigations, complex digital forensic collections, network vulnerability and rapid security assessments. Andrew also consulted on global matters relating to information security, digital forensics and e-discovery with Kroll's Secure Information Services and Computer Forensic Consulting Practice. He also developed and implemented new client service offerings relating to incident response protocols and plan development, electronic data collection practices and policy review, digital forensic laboratory assessment, and wireless network vulnerability analysis.

Further, his previous employment experience includes overseeing senior level e-discovery, digital forensic investigations, incident response and information security functions at CIGNA Healthcare. In this role, Andrew assessed and implemented new policies and procedures pertaining to digital evidence preservation, collection and storage in accordance with accepted industry practices. He was also charged with ensuring that confidential information was protected during storage and transmission relating to the daily operations of this global organization.

As a former supervisory forensic analyst and Special U.S. Marshall with the Regional Electronic & Computer Crime Task Force (REACCT), he managed digital-related investigations on all types of media, ensured compliance with accepted computer forensic protocols, and presented testimony for numerous criminal cases related to computer crime and digital forensics. Andrew has also lectured across the country on topics relating to computer crime investigations, information security, data privacy and digital forensics for target audiences at all professional levels across various business industries.

Deposition and expert testimony

- *Talon Transaction Technologies, Inc. & Nexpay, Inc. v. StoneEagle Services, Inc.,* United States District Court, Northern District of Texas, Dallas Division. Case No. 3:13-CV-00902-D. April 2015.
- *KPMG, LLP v. Ronald B. Harvey,* State of New York. Arbitration Proceeding. July 2012.
- *Hispano USA, LLC v. Azteca Milling, LP and Gruma Corporation v. Javier Ruiz Galindo,* State of Texas, District Court of Bexar County, 288 Judicial Court. Case No. 2011-CI-01313. May 2012.
- *Passlogix v. 2FA Technology, et al.,* United States District Court, Southern District of New York, New York City. Case No. 08-CV-10986. January 2010.
- *Leor Exploration and Production, et al. v. Guma Aguiar,* United States District Court, Southern District of Florida, Miami Division, Florida. Case No. 09-60136-CIVIL-SEITZ. December 2009. Evidentiary Hearing.
- *Passlogix v. 2FA Technology, et al.,* United States District Court, Southern District of New York, New York City. Case No. 08-CV-10986. November 2009.
- *Leor Exploration and Production, et al. v. Guma Aguiar,* United States District Court, Southern District of Florida, Miami Division, Florida. Case No. 09-60136-CIVIL-SEITZ. October 2009. Evidentiary Hearing.
- *Skanska USA Building Inc. v. Long Island University, et al.,* Supreme Court, Kings County, New York. Index No. 15097/2006. June 2009.
- Substantial experience providing testimony in the following types of proceedings: Motions, Depositions, Grand Jury, Hearings, Bench and Jury Trials
- Testifying experience is estimated to be in excess of 500 civil and criminal case appearances.

Selected technical/professional presentations

- PLUS Annual Conference 2015, “Handling Cross Boarder Data Breaches”, Dallas, Texas, November 2015
- NetDiligence Annual Cyber Claim Study 2015, “The Real Cost of a Data Breach”, Webinar, November 2015
- NetDiligence Cyber Risk & Privacy Liability Forum, “Leveraging Human Stupidity: Hackers’ Approach to Obtaining Crown Jewels,” Santa Monica, California, October 2015
- IAPP Privacy. Security. Risk. Conference. “NetDiligence Cyber Claims Study. The Real Cost of a Data Breach”, Las Vegas, Nevada, October 2015
- Chase Cyber Security Conference, “Data Breach Readiness”, Woburn, Massachusetts, September 2015
- RSM Insurance Industry, “Prevent, detect and correct: Cybersecurity and data breach preparedness”, Webinar, September 2015
- RSM Law Firm CIO Conference, “Security & Privacy Trends,” Chicago, Illinois, June 2015
- Net Diligence Cyber Risk & Privacy Liability Forum, “Leveraging Human Stupidity: Hackers’ Approach to Obtaining Crown Jewels,” Philadelphia, Pennsylvania, June 2015

- Security & Privacy Trends, “Security Controls, Incident Response, & Mitigating Risk,” London, United Kingdom, May 2015
- Advisen Ltd, “The Changing Face of Cyber Risk,” Webinar, April 2015
- E&I Corporate Services, “Lessons from the Dark Side: What We Can Learn from a Data Breach,” Webinar, March 2015
- American Apparel & Footwear Association, “Security & Privacy,” Webinar, March 2015
- Microsoft Transparency & Trust in the Cloud, “Cloud Security Best Practices,” Boston, Massachusetts, March 2015
- RSM Cyber Security Series, “Part 3: Corrective Controls,” Webinar, March 2015
- Net Diligence Annual Cyber Claim Study 2014, “The Real Cost of a Data Breach,” Webinar, January 2015
- Construction Financial Management Association, “Managing Enterprise Risk for Your Growing Construction Company,” Boston, Massachusetts, January 2015
- Law Technology News, “Computer Networks & Business Partnerships: Protecting the Exchange of Data,” Cybersecurity & Data Protection Legal Summit, New York, New York, December 2014
- Greater Miami Chamber of Commerce, “The Convergence of Technology & Banking: Security & Compliance,” Miami, Florida, November 2014
- RSM M&A Learning Exchange, “Addressing IT Risks in the Private Equity Environment,” Chicago, Illinois, November 2014
- RSM CFO Roundtable, “Data Breach Readiness & Response,” New York, New York, November 2014
- Community College of Rhode Island, “Data Breach Readiness and Response Planning,” Security Awareness Day, Warwick, Rhode Island, October 2014
- Massachusetts Bankers Association & Financial Managers Society, “Data Breach Readiness and Response Plan,” Finance & Accounting Conference, Boston, Massachusetts, October 2014
- Infovest Security & Regulatory Issues for Hedge Funds, “Impact of Cyber Security Threats On the Hedge Fund Industry,” Stamford, Connecticut, October 2014
- RSM Financial Services, “What Hedge Funds Need to Know About Cybersecurity Today,” Online Video Recording, October 2014
- RSM 2014 Investment Industry Summit, “Cybersecurity Discussion,” New York, New York, September 2014
- RSM Emerging Technology Conference, “Data Breach Readiness & Response,” Minneapolis, Minnesota, September 2014
- RSM Emerging Technology Conference, “Data Breach Readiness & Response,” Boston, Massachusetts, September 2014
- MHBT, “It’s 3AM - Do you know where your data is?,” Dallas, Texas, September 2014
- Beazley, “Data Breach/Information Security Readiness,” Webinar, August 2014
- RSM Public Sector Industry, “Security Threats & Remediation Strategies,” Webinar, August 2014
- Pennsylvania Bar Institute, “Cybersecurity Law 101—Perspectives from Government and Academia,” Philadelphia, Pennsylvania, August 2014
- Premier Insurance Webinar, “Forensic Investigation Best Practices & Pitfalls,” August 2014
- Massachusetts Council of Presidents CFO Joint Meeting, “Data Breach Readiness & Response,” Hyannis, Massachusetts, June 2014
- ISACA New England IT Audit/Security Annual Meeting, “How Organizations Can Stay Relevant and Secure Through Innovative Technology,” Boston, Massachusetts, June 2014
- RSM Tax Controversy Webinar, “IRS Account Problems: Preventing Identity Theft and Managing IRS Penalties and Interest,” May 2014

- FMI Financial Executive & Internal Auditing Conference, “Information Security & Privacy: Are You Ready For A Data Breach?,” San Francisco, California, May 2014
- New England Board of Higher Education, “Cyber Defense: Executive and Board Leadership Strategies for Assessing Threats, Preventing Security Breaches and Promoting University Awareness,” Boston, Massachusetts, April 2014
- Boston Chapter of the Association of Government Accountants, “Data Privacy & Security,” Greater Boston, Massachusetts, March 2014
- Annual Boston Nonprofit Summit, “How Nonprofits Can Stay Relevant and Secure Through Innovative Technology,” Boston, Massachusetts, March 2014
- ISACA Boston Breakfast Meeting, “Information Security & Privacy: Overview of Data Breach Readiness & Response,” Boston, Massachusetts, March 2014
- UHC Web Conference—Best Practices for the “First Responder” IT Professional to a Breach Incident, “Data Breach Readiness & Response,” March 2014, Webinar
- Corporate Counsel & Compliance Exchange, “Strengthening Your Anti-Corruption Compliance Program,” Palm Springs, California, February 2014
- Massachusetts Attorney General’s Office, “Search Strategies: Finding What You Want in the eDiscovery Pile,” Boston, Massachusetts, October 2013
- Boston University School of Law, “E-Discovery Law & Practice,” Guest Lecturer, Boston, Massachusetts, September 2013
- RIMS 2013 Florida Chapters 38th Annual Joint Educational Conference, “Network Security & Privacy—Emerging Trends,” Naples, Florida, July 2013
- National Underwriter Property & Casualty, “Got Cyber Coverage? Strategies to Protect Your Clients,” Property Casualty 360, Online Webinar, May 2013
- Premier Insurance Management Services, “Data Encryption—A Critical Loss Mitigation Tool for Healthcare Organizations,” Online Webinar, April 2013
- New Jersey Institute for Continuing Legal Education, “Mastering Data Breach, ID Theft & Privacy Laws,” Rutgers University Law Center, New Brunswick, New Jersey, March 2013
- Wyatt & Wells Fargo Seminar, “Network Security, Privacy, & Risk,” Louisville, Kentucky, January 2013
- PLUS 25th Annual Conference, “Privacy & Data Security: The True Impact of Exposures,” Chicago, Illinois, November 2012
- Net Diligence Cyber Risk & Privacy Liability Forum, “Why Can’t We All Just Stop Breaches!,” Marina del Ray, California, October 2012
- Beazley Bytes, Connecting the Dots—Forensic Services, Podcast, October 2012
- Changes to European Data Privacy Changes Everything, 2012 Connecticut Privacy Forum, Hartford, Connecticut, October 2012
- Cloudy with a Chance of a Perfect Storm: Discovery in the Cloud Computing Age, American Bar Association, ABA Annual Meeting, Chicago, Illinois, August 2012
- Cybercrime Workshop: Computer Investigations 101: No IT Experience Required, ASIS—Boston Chapter, Boxborough, Massachusetts, April 2012
- ALPFA Law—Privacy and Information Security Landscape in the Wake of Wikileaks, ALPFA Boston and ALPFA Law Board, April 2011
- Social Networking, Data Warehouses and Digital Cultures, Ohio Association of Chiefs of Police In-Service Training, Columbus, Ohio, 2010

Selected articles/publications

- Using Data Analytics to Detect and Prevent Fraudulent Activity, Risk & Compliance Magazine, July–September 2015
- RSM Incident Response Guide, April 2015
- Successfully Vetting Forensic Firms, Risk & Compliance Magazine, April–June 2015
- Five Tips to Enhance Your Organization's Cybersecurity, Boston Business Journal, March 2015
- Five Tips to Enhance Your Organization's Cybersecurity, High Profile Magazine, February 2015
- Bookity, "The Art of Data Security for Museums," February 2015
- RSM Investment Industry Insights, "Cybersecurity & Hedge Funds," October 2014
- Implementing a proactive data security plan: The 3 stages of a data breach, RSM Insight Article, September 2014
- Risk Managers, Lawyers, & Information Technology: Three Different Languages, One Common Goal, NAVIGANT Experts Corner, November 2012
- Tweet, Post, & Read All About Me: A Discussion on Technology, Social Networking, & the Workplace, OACP Magazine, 2010
- Digital Mayhem in Schools, Author, Omni Publishing Company, 2007
- Email Investigations and Instant Message Tracking, Author, Omni Publishing Company, 2007
- Preserving Digital Evidence, Author, Omni Publishing Company, 2007
- Digital Forensic Investigations, Author, Omni Publishing Company, 2006

Professional affiliations

- Institute of Internal Auditors (IIA), 2014–Present (member)
- Information Systems Audit and Control Association (ISACA), 2013–Present (member)
- International Association of Privacy Professionals (IAPP), August 2012–Present (member)
- High Technology Crime Investigation Association, 2004–Present (member)
- High Technology Crime Consortium, 2002–Present (member)

Professional certifications

- Certified Information Systems Security Professional (CISSP)—International Information Systems Security Certification Consortium (ISC)[2]
- Certified Information Security Manager (CISM)—ISACA
- PCI Security Standards Council LLC Qualified Security Assessor (QSA)
- EnCase® Certified Examiner, (EnCE®) in EnCase® Forensic Edition
- SANS GIAC Security Essentials (GSEC)
- National Security Agency (NSA) Information Security Professional

Education

- Master of Science, national security, University of New Haven
- Graduate certificates in computer forensic investigations and information security, University of New Haven
- Bachelor of Science, criminal justice, Anna Maria College

Rusty Yeager
HealthSouth Corporation

3660 Grandview Parkway, Suite 200, Birmingham, AL 35243, USA
205.969.6645
Rusty.Yeager@healthsouth.com
www.healthsouth.com/

Rusty Yeager is Senior Vice President and Chief Information Office at HealthSouth and has more than 25 years of healthcare information technology experience and over 15 years of increasing responsibilities in information technology leadership at HealthSouth. Additionally, he served as a Medical Service Corps officer specializing in healthcare information technology in the United States Air Force for 20 years.

Yeager holds a Master's in business administration from the University of Texas at San Antonio, a Bachelor's in marketing from Texas A&M University-Kingsville and an executive certificate in management and leadership from MIT's Sloan School of Management. Rusty has been named as one of “Ones to Watch” by *CIO magazine* and HealthSouth's Information Technology Group was named to the magazine's "Top 100" list for the implementation of its Beacon business intelligence and reporting system.

He is a member of numerous professional organizations including the College of Healthcare Information Management Executives (CHIME) and is a senior member of the Healthcare Information and Management Systems Society (HIMSS). He also holds or has held numerous IT and IT security certifications or credentials.

- HealthSouth is one of the nation’s largest providers of post-acute healthcare services, offering both facility-based and home-based post-acute services in 34 states and Puerto Rico through its network of inpatient rehabilitation hospitals, home health agencies, and hospice agencies.

India E. Vincent

Intellectual Property, Mergers & Acquisitions, Business & Succession Planning, Non-Compete & Trade Secrets, Commercial Contracts, Corporate Law, Intellectual Property Litigation, Cybersecurity and Data Privacy

Birmingham, Alabama
ivincent@burr.com
Phone: (205) 458-5284
Fax: (205) 244-5714

Paralegal: Paula Kustos
(205) 458-5131
pkustos@burr.com

Legal Secretary: Karen Williams
(205) 458-5329
kwilliams@burr.com

About India E. Vincent

India's practice is devoted to helping clients identify, protect and generate maximum value from their intellectual property and their data.

India's areas of practice include intellectual property, technology, business planning, and corporate transactions. She assists her clients in creating, developing, growing, managing and selling their businesses with a specific focus on maximizing the value of their intellectual property assets. As part of those efforts, India works with clients to determine appropriate strategies for protecting, licensing and enforcing their intellectual property, including trademarks, service marks, patents, trade secrets, and copyrights, and advises clients regarding contractual relationships with customers and vendors.

India works with clients in all industries, including the software, technology, biotechnology, entertainment, health care, and manufacturing industries. India also assists clients with developing security and data protection polies and breach response plans.

Education

- J.D., Samford University, Cumberland School of Law (1999)
- MIMSE, North Carolina State University (1993)
- B.S., ECE, Clemson University (1992)

Professional Associations

- International Trademark Law Association,
  Emerging Issues Committee (2014 - 2015); Data Privacy Committee (2016-2017)
- American Intellectual Property Law Association (AIPLA), Electronic & Computer Law Committee and Women in IP Law Committee
- American Bar Association
- Alabama Bar Association
- Birmingham Bar Association
- Georgia State Bar Association

Representative Matters

- Manage trademark portfolios for multiple clients including, assisting with selection and clearance of marks, registration of marks, and advising on defending and enforcing such marks.
- Advise start-up and growth companies on investment strategies, IP protection strategies, and other matters relevant to an emerging company.
- Represent franchise companies in the development of their brand strategies, including registration, protection and enforcement of their marks.
- Assist large manufacturing companies in the negotiation of development and licensing agreements for their manufacturing software systems.
- Represent consumer and business-to-business based brand companies in all business matters.
- Assist large industrial clients in development of copyright and trademark policies.
- Assist clients in development of proactive cyber-security policies and breach response plans.

Honors & Awards

- *Best Lawyers in America,* Copyright Law, Trademark Law (2012-2016)
- *Best Lawyers in America*, "Lawyer of the Year," Trademark Law, Birmingham, Alabama (2015)
- Business Journal's "Top 40 Under 40" (2009)

Licensed In

- Alabama
- Georgia

Admitted In

- US Patent and Trademark Office

Community Involvement

- Birmingham Venture Club, Board Member
- Alabama Launchpad (*an initiative of the Economic Development Partnership of Alabama to foster start-up business in Alabama*)
- TechBirmingham, Executive Board Member
- AIM Group / CAAN (*Angel Investor Management group / Central Alabama Angel Network*)