

INSIDE: New Threats Compromise Data Safety • How Competence Requirements Affect Your Practice • And More

Delaware Lawyer

A PUBLICATION OF THE
DELAWARE BAR FOUNDATION



VOLUME 34 ♦ NUMBER 4
\$3.00 ♦ WINTER 2016-2017

DATA SECURITY:

Tips for Mobile Devices,
Social Media, eMail & Courtroom Technology

Nonprofit Organization
U.S. Postage
PAID
Wilmington, Delaware
PERMIT NO. 697

LET US CATER TO YOU

Janssen's Market offers customized, full-service catering, event planning, party rentals, floral arrangements, and more. From breakfast and lunch for 6 to a cocktail party for 50, we can deliver all of your needs to the office, hotel, or wherever you are working!

Contact our catering director today at 302.654.9941 x3

3801 Kennett Pike • Greenville, DE 19807
www.janssensfinefoods.com



DELAWARE LAWYER BUSINESS PROFILES



Q&A

Ted Carlson, Gunnip & Company LLP

Bringing more than 30 years of experience dealing with trust, estate, gift and personal income tax issues, Ted recently joined Gunnip & Company. Ted feels that he brings the most value by frequently collaborating with Trust and Estate attorneys on the implementation of a client's estate plan.

What lead you to accounting?

I have always been fairly quick with numbers and solving problems. The balancing of debits and credits made sense. I quickly gravitated towards taxation and have concentrated on that my entire career.

What are the biggest changes you have seen the last 30 years? What has not changed during that time?

The 1986 Tax Act which was a major overhaul that happened right at the beginning of my career, and the advancement of computer technology. The thing that has never changed is that debits must equal credits.

You have worked with many attorneys and law practices. What do you enjoy about these relationships?

I enjoy having in depth conversations in order to leverage each other's

expertise in order to solve problems.

It is very rewarding when you devise a plan, implement it, and then watch it work, correctly.

What support can you provide a Trust and Estate Attorney?

There are several ways to complement an attorney's services with our expertise. I can provide support and guidance for client's estate, trust, gift, and transfer tax plans. I also enjoy working with the attorney and the executor to help them understand the income tax process. I believe in planning early, revisiting the plan regularly and not defending the status quo.

What might your clients be surprised to know about you?

I am not just a tax geek; I enjoy driving my Corvette, fairly quickly.

**Specializing in
Tax Planning and
Compliance for
Trusts, Estates,
and Individuals**

Experience + Longevity

Dependability to help you build a secure foundation.

Business Tax Planning and Preparation • Audit, Review and Compilation Services
Trust, Estate and Gift Taxes • Individual Tax Planning and Preparation
Bookkeeping, Payroll and Controllorship Functions
Nonprofit, Government and EBP Audits

Gunnip & company LLP
Certified Public Accountants and Consultants



EXPERIENCE IS THE DIFFERENCE®

302.225.5000 | GUNNIP.COM

Delaware Lawyer

CONTENTS



WINTER 2016/2017

EDITORS' NOTE 6

CONTRIBUTORS 7

FEATURES 8

**It's 'Ready, Set, Go':
Cyber Threats to Lawyers Grow**

The Data Security Leading Practice Group

**14 Learning to Cope
with Technology Competence Requirements**

The Basic Skills and Social Media Leading Practice Groups

18 Cybersecurity Implications in e-Discovery

The eDiscovery Leading Practice Group

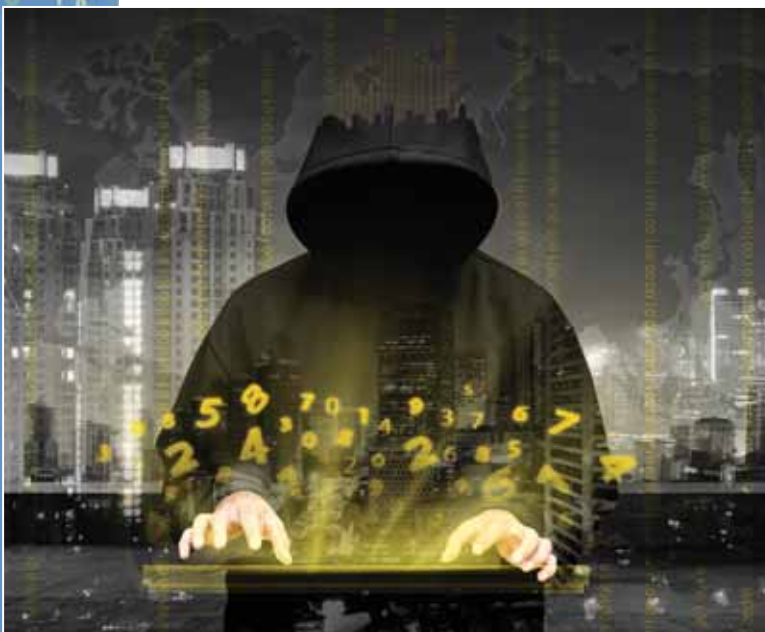
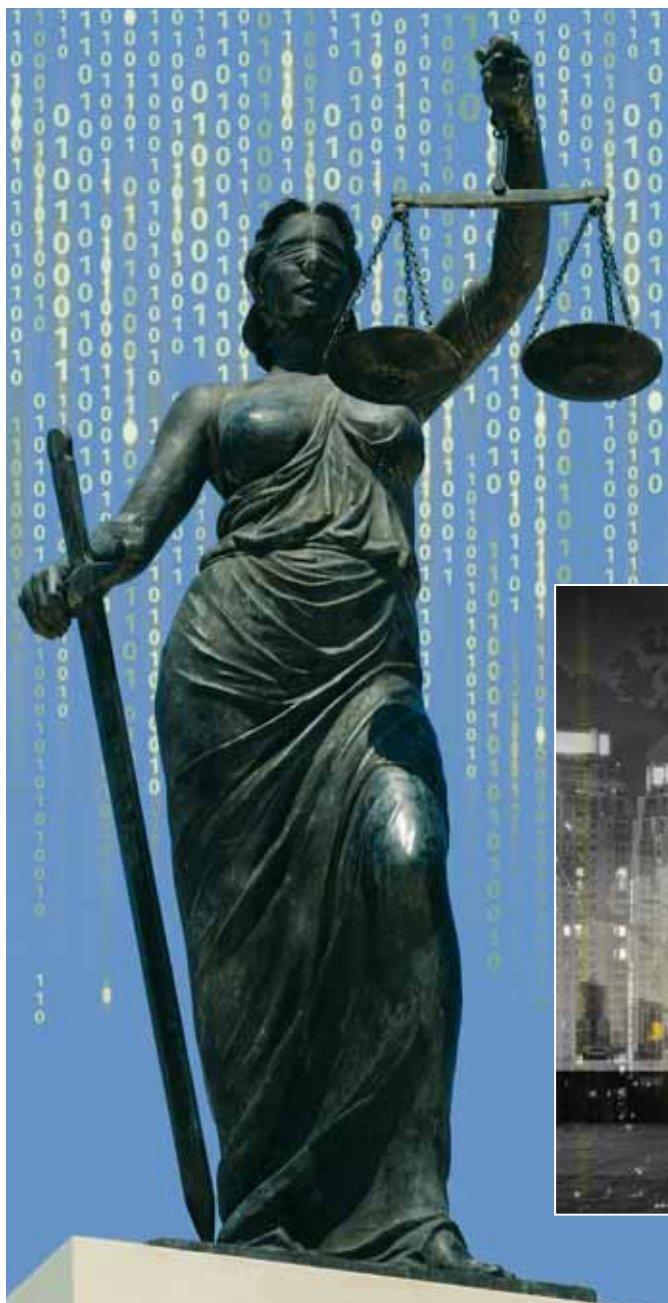
22 Email Technology, Security and Privacy

The eMail Leading Practice Group

24 Wi-Fi in the Courtroom

The Courtroom Technology Leading Practice Group

28 OF COUNSEL: Judge Steven L. Butler






Sheraton Suites is where colleagues *gather.*

Bring the best minds together in our Full-Service Legal Suites & Meeting Facilities. Located in downtown Wilmington within minutes of the Courthouse, the beautiful Wilmington Riverfront & Amtrak Station. Easily accessible to the I-95 Corridor and the Philadelphia Airport.

We are the experts in handling all Mock Trials. The Sheraton Suites offers 3 fully furnished Legal Office Suites with 3,900 SF that feature:
21 Workstations • Voicemail & T-1 Connections • LAN Network Capabilities • 2 Conference Areas • Storage Space • Built-in Kitchen Areas

 Sheraton.com/suiteswilmington



Sheraton®

SUITES
WILMINGTON
DOWNTOWN

Amenities:

- 223 Spacious Suites
- 7,600 SF of Flexible Meeting Space
- Customized Catering Menus
- On-Site Parking
- Shuttle Service
- Full Service Restaurant & Lounge
- Indoor Pool & Fitness Center



422 Delaware Avenue Wilmington, DE 19801
P 302.576.8040 | Eltreu@sheratonwilmington.com

© 2016 Starwood Hotels & Resort Worldwide, Inc. All Rights Reserved. Sheraton and its logo are the trademarks of Starwood Hotels & Resorts Worldwide, Inc. or its affiliates.

LIKE A GOOD WINE, KRESTON'S
HAS THE BENEFIT OF AGE

Celebrating 84 Years



BEST
WINE STORE

KRESTON
WINE & SPIRITS

Same Family, 4 Generations, Since 1933
Best Service. Best Selection. Best Price.

904 Concord Ave. (Concord & Broom)
Open 7 days a week
302.652-3792

Middletown Crossing Shopping
Open 7 days a week
302.376-6123

www.krestonwines.com

BRIGGS
AUCTION, INC.
SINCE 1932

BriggsAuction.com
1347 Naamans Creek Road
Garnet Valley, PA 19060
610.566.3138

Comprehensive Estate Liquidation Services

SPECIALIZING IN LOCAL ESTATES FOR 85 YEARS

WEEKLY ESTATE AUCTIONS

FINE CATALOG & SPECIAL COLLECTIONS

ESTATE APPRAISALS | REAL ESTATE AUCTIONS



Reichert Estate, Wilmington, DE
Sold for \$800,000

Delaware Lawyer

A publication of Delaware Bar Foundation
Volume 34 Number 4

BOARD OF EDITORS

Chair:

Charles J. Durante
Hon. Thomas L. Ambro
Lawrence S. Drexler
Dominick T. Gattuso
Amy C. Huffman
Kate S. Keller
Rosemary K. Killian
James H.S. Levine
Richard A. Levine
David C. McBride
Elena C. Norman
Karen L. Pascale
Blake Rohrbacher
Jeffrey M. Schlerf
Gregory W. Werkheiser
Robert W. Whetzel
Hon. Loretta M. Young

DELAWARE BAR FOUNDATION

100 W. 10th Street / Suite 106
Wilmington, DE 19801
302-658-0773 / 302-658-0774 (fax)

BOARD OF DIRECTORS

President:

Jenness E. Parker
Ryan C. Cicoski
C. Malcolm Cochran, IV
Kelly E. Farnan
Michael Houghton
Kathi A. Karsnitz
Elizabeth M. McGeever
Hon. Laurie Selber Silverstein
Benjamin Strauss
William H. Sudell, Jr.
Hon. Karen L. Valihura
Jeffrey A. Young

Executive Director:

Melissa W. Flynn

DELAWARE LAWYER

is produced for the
Delaware Bar Foundation by:

Today Media Custom Communications
3301 Lancaster Pike, Suite 5C
Wilmington, DE 19805

Chairman: Robert Martinelli

President/Editor: Jonathan Witty

Art Director: Samantha Carol Smith

Subscriptions orders and address changes, call:
Jen Schuele, 302-656-1809

Advertising information, call:

Jessica Stryker, 302-504-1365
jessica.stryker@todaymediacustom.com

Delaware Lawyer is published by the Delaware Bar Foundation as part of its commitment to publish and distribute addresses, reports, treatises and other literary works on legal subjects of general interest to Delaware judges, lawyers and the community at large. As it is one of the objectives of *Delaware Lawyer* to be a forum for the free expression and interchange of ideas, the opinions and positions stated in signed material are those of the authors and not, by the fact of publication, necessarily those of the Delaware Bar Foundation or *Delaware Lawyer*. All manuscripts are carefully considered by the Board of Editors. Material accepted for publication becomes the property of Delaware Bar Foundation. Contributing authors are requested and expected to disclose any financial, economic or professional interests or affiliations that may have influenced positions taken or advocated in the articles. That they have done so is an implied representation by each author.

Copyright 2017 Delaware Bar Foundation
All rights reserved, ISSN 0735-6595



Delaware Back Pain & Sports Rehabilitation Centers

Depend on us to get you better faster.



BOARD-CERTIFIED PHYSICAL MEDICINE & REHABILITATION SPECIALISTS, INTERVENTIONAL PAIN MANAGEMENT SPECIALISTS, AND CHIROPRACTIC CARE

Physical Medicine & Rehabilitation/EMG

Barry L. Bakst, D.O., FAAPMR
Craig D. Sternberg, M.D., FAAPMR
Arnold B. Glassman, D.O. FAAPMR
Stephen M. Beneck, M.D., FAAPMR
Lyndon B. Cagampan, M.D. FAAPMR
Jeffrey S. Meyers, M.D., FAAPMR

Pain Management Counseling

Irene Fisher, Psy.D.

Physical Medicine & Rehabilitation/EMG/

Certified Brain Injury Medicine

Anne C. Mack, M.D., FAAPMR

Interventional Pain Management

Pramod K. Yadhati, M.D.

Interventional Plan Management/PMR/EMG

Rachael Smith, D.O., FAAPMR
Kartik Swaminathan, M.D., FAAPMR

Chiropractic Care

Kristi M. Dillon, D.C.
Brian S. Baar, D.C.
Marjorie E. Mackenzie, D.C.
Adam L. Maday, D.C.
Scott Schreiber, D.C., DACRB
Mark Farthing, D.C.
Hetel Patel, D.C., FIAMA
Ty Harmon, D.C.
Jennifer Walder, D.C.

Unique Services Include: Certified Brain Injury Medicine • Platelet Rich Plasma Therapy (PRP) • Acupuncture • EMG/NCS
Ultrasound Guided Musculoskeletal Injections • Prolotherapy • Anti-Gravity Treadmills • Cold Laser Therapy • QFCes
Rehabilitation Therapy • Psychology/Pain Management Counseling

ACCEPTING NEW MOTOR VEHICLE & WORKERS' COMPENSATION CASES DEPARTMENT OF TRANSPORTATION PHYSICAL EXAMS

Workers' Comp Certified Providers & Private insurances accepted

www.delawarebackpain.com



Foulk Road Park Office
Riverside Office
Omega Professional Center
Glasgow Medical Center
NEW!!! Middletown
Smyrna Office
Eden Hill Medical Center

2006 Foulk Road, Suite B, Wilmington, DE 19810 • 302.529.8783 • Fax-302.529.7470
700 Lea Boulevard, Suite 102, Wilmington, DE 19802 • 302.764.0271 • Fax-302.762.4076
87 Omega Drive, Building B, Newark, DE 19713 • 302.733.0980 • Fax-302.733.7495
2600 Glasgow Avenue, Suite 210, Newark, DE 19702 • 302.832.8894 • Fax-302.832.8897
124 Sleepy Hollow Dr., Ste. 204, Middletown, DE 19709 • 302.376.8080 • Fax-302.378.1684
29 N. East Street, Smyrna, DE 19977 • 302.389.2225 • Fax-302.389.1003
200 Banning Street, Suite 350, Dover, DE 19904 • 302.730.8848 • Fax 302.730.8846

EDITORS' NOTE

Kevin F. Brady and Richard K. Herrmann

Hardly a day goes by without a news story about a data breach or a cyberattack. This past year was hyperactive with notorious hacks ranging from the attack on the Democratic National Committee's email server, W-2 information at federal agencies including the Federal Insurance Deposit Corporation, the Department of Homeland Security and the Internal Revenue Service, as well as healthcare organizations and social media sites like LinkedIn.

This is an unsettling time for individuals and corporations when it comes to data privacy and security issues — and the bad news is that things are getting worse. According to the Identity Theft Resource Center, there were almost 1,000 reported security breaches in 2016, exposing over 35 million records (that number does not include breaches that did not report the number of records that were compromised or undiscovered breaches).

From 2015 to 2016 there was a 300% increase in the number of ransomware attacks (including attacks on Delaware law firms) and that trend shows no signs of slowing down. These stories cause anxiety and even panic in all of us. While attacks are becoming more innovative, invasive and sophisticated, some of the most successful attacks are quite simple.

What should we do? How can we protect ourselves? Attack-

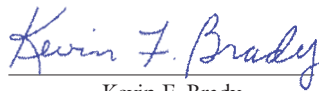
"Hackers find more success with organizations where employees are under appreciated, over worked and under paid. Why would anyone in an organization like that care enough to think twice before clicking on a phishing email?"

— James Scott, Sr. Fellow,
Institute for Critical Infrastructure Technology

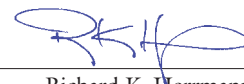
ers are likely to continue to use social engineering and social networks to target sensitive roles or individuals within an organization and seek to obtain their data. Social media and endpoint computing devices like smartphones and tablets will remain the weak spots in many organizations' security structure.

The near-term growth of the "Internet of Things" with robots, drones and autonomous vehicles will only increase the dangers of cyberattacks. Machine learning, artificial intelligence, virtual and augmented reality, intelligent apps — the list goes on and on. From a personal standpoint, how can you protect your data? From a legal perspective, how can you protect your clients' data?

What follows in this edition of *Delaware Lawyer* is an exploration by members of the Delaware Supreme Court's Commission on Law & Technology of how pervasive cybersecurity issues can be. We hope that this foray into the minds of cybercriminals, hacktivists and terrorists will be of value to every member of the Delaware Bar in terms of maintaining privacy and protecting client confidences.



Kevin F. Brady



Richard K. Herrmann

The Delaware Bar Foundation is pleased to announce

THE BRUCE M. STARGATT LEGAL ETHICS WRITING COMPETITION



This writing competition is made possible by a generous gift to the Delaware Bar Foundation from Mrs. Barbara Stargatt and her family in memory of her late husband, Bruce M. Stargatt. Bruce was a distinguished Delaware lawyer who, among many other accomplishments, was a founding partner of Young, Conaway, Stargatt & Taylor, and a past president of the Delaware Bar Foundation and the Delaware State Bar Association.

In keeping with Bruce Stargatt's keen interest in legal writing and the ethical practice of law, we invite papers concerning ethical issues in the practice of law. Beyond this general description, the precise issue to be dealt with is at the author's discretion.

Please visit www.delawarebarfoundation.org/stargatt-writing-competition
for additional details including eligibility requirements and submission date.

THE DELAWARE SUPREME COURT COMMISSION ON LAW AND TECHNOLOGY

This issue of *Delaware Lawyer* has been a collaborative effort of the entire Commission, the members of which are briefly listed below. Each is a member of one or more of the following Working Groups: The Bench Perspective, Data Security, Mobile Technology, Basic Skills, Social Media, eMail, eDiscovery, Courtroom Technology and The Cloud.

COMMISSION MEMBERS

The Honorable James T. Vaughn, Jr.

is the Supreme Court Liaison to the Commission. Justice Vaughn was appointed Resident Judge in Kent County of the Superior Court of Delaware in 1998, President Judge of the Superior Court in 2004 and Justice of the Supreme Court in 2014.

The Honorable J. Travis Laster

was sworn in as Vice Chancellor of the Court of Chancery in 2009. Prior to his appointment, he was one of the founding partners of Abrams & Laster LLP.

The Honorable Eric M. Davis

became a Judge of the Superior Court in 2012. He previously served as a Judge on the Court of Common Pleas of Delaware, beginning in 2010.

The Honorable Michael K. Newell

was appointed Chief Judge of the Family Court in 2015. Prior to his appointment, Chief Judge Newell served as a Family Court Judge since 2004.

The Honorable Kenneth S. Clark, Jr.

was appointed to the Court of Common Pleas in 2000.

Kevin F. Brady

is Of Counsel with Redgrave LLP.

Vincent M. Catanzaro

is Of Counsel with Shook Hardy and Bacon.

Diane M. Coffey

is a partner of Marc J. Bern & Partners LLP.

Margaret M. DiBianca

is Counsel with Young Conaway Stargatt & Taylor, LLP.

Ann Shea Gaza

is a partner with Young Conaway Stargatt & Taylor, LLP.

Douglas D. Herrmann

is a partner with Pepper Hamilton LLP.

Richard K. Herrmann

is a partner with Morris James LLP.

Bruce E. Jamison

is a director of Prickett, Jones & Elliott, P.A.

Brian S. Legum

is an associate of Kimmel, Carter, Roman, Peltz & O'Neill, P.A.

Sean P. Lugg

is State Prosecutor for the Delaware Department of Justice.

Steve Martin

is the Chief Information Officer of Potter Anderson Corroon LLP.

George A. Massih, III

is Chief Legal Office and General Counsel of Corporation Service Company, Inc.

Edward J. McAndrew

is a partner in Ballard Spahr LLP.

Ryan P. Newell

is a partner in Connolly Gallagher LLP.

The Honorable Donald F. Parsons

is Senior Counsel with Morris Nichols Arsht & Tunnell.

Gilbert L. Pinkett

is Chief Information Officer at Maron Marvel Bradley Anderson & Tardy LLC.

The Honorable Henry DuPont Ridgely

is Senior Counsel with DLA Piper.

Thomas Russo, Jr.

is President of DoeLegal.

Thomas L. Sager

is a partner in Ballard Spahr LLP.

Rodney A. Smolla

is the Dean of Delaware Law School.

William S. Stone

is Chief Information Officer at Morris James LLP.

It's 'Ready, Set, Go': Cyber Threats to Lawyers Grow

As data security breaches escalate, attorneys develop strategies to minimize risk, protect client confidentiality and deal with the worst scenarios.

Political campaign hacks, where the other shoe seems to keep dropping. 'Internet of Things' botnet attacks, where the Internet goes dark on the East Coast. Data breaches that dwarf those of days past in size, scope and impact. Cleverly spoofed emails that trick others into dispersing funds or disclosing confidential data. Thousands of ransomware attacks daily that reduce data and devices to cyber bricks.

For lawyers in organizations of all sizes, 2016 may be remembered as the year in which cyber threats broke into public view. The largest data breach (by amount of data lost) now belongs to a law firm, and is simply known as "The Panama Papers." Hackers openly discussed targeting large firms on underground forums.

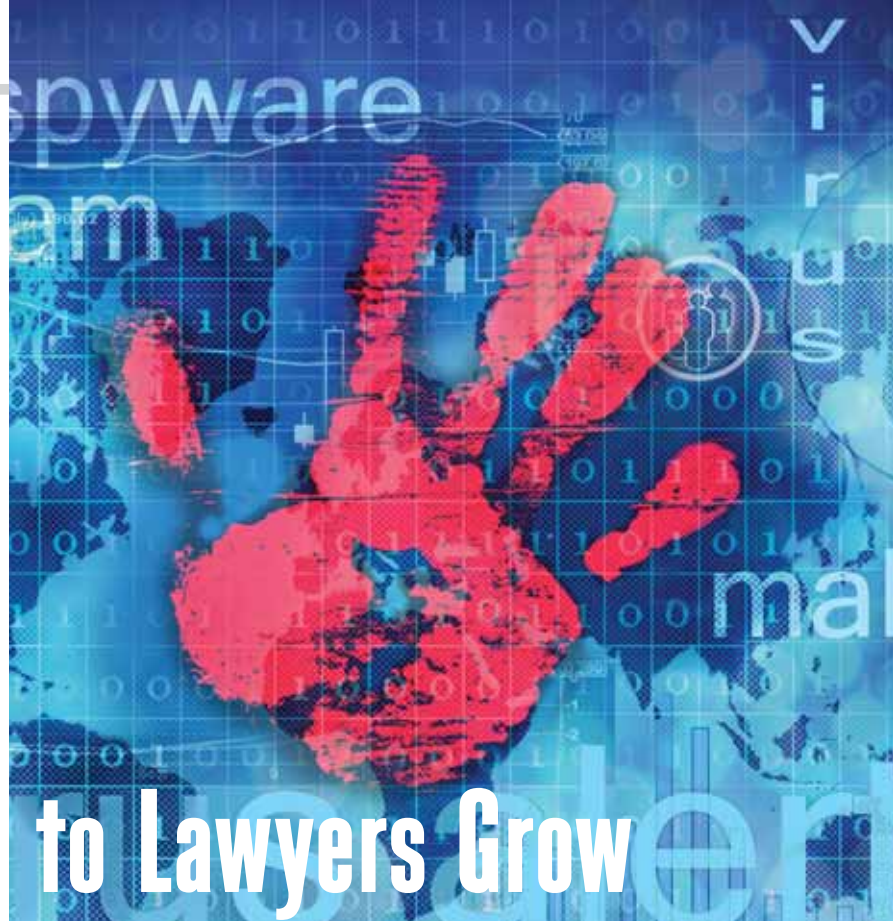
Some firms — large and small — publicly acknowledged suffering data breaches and other cyber incidents. Some became embroiled in litigation tied to cybersecurity issues. Others saw employees prosecuted for insider data theft or investigated as a result of leaked data. At least one boutique cited cybersecurity concerns as a reason for merging with a larger firm. More and more lawyers received questionnaires and audit requests from clients concerned about cybersecurity.

In-house counsel have their hands full as well. According to Kaspersky Labs, 90

percent of businesses have experienced a cyberattack. The Ponemon Institute has pegged the global average cost of a data breach at \$4 million, *excluding regulatory, legal and reputational costs*. Despite it all, many firms and in-house legal departments cite "data security" as a hot, new practice area.

Whether one plays the role of client, counsel or both, these trends are impacting all organizations and lawyers. Confidentiality and discretion in handling a client's most pressing and sensitive matters is our stock in trade. Unfortunately, confidentiality and discretion are under cyber assault — as destroying reputations, altering business and legal strategies, disrupting operations and eroding public confidence have joined illicit financial gain as primary objectives of cyber actors.

The most pressing question in our new cyber reality is not if, when or who,



but what threat comes next?

A Shifting Landscape for In-house Counsel

Among the expanding list of issues facing the general counsel today, data security has become a chief concern for their corporations and boards of directors.¹ This threat has placed in-house counsel at the center of a virtual war on a new battlefield. Yet, unlike traditional legal risks to the corporation, attacks on the company's infrastructure and data require new, multi-dimensional and technically sophisticated defenses.

What makes security so unique and difficult to address is the ever-evolving nature of attacks and breaches, creating a moving target that calls for expertise beyond the legal department, including IT, human resources, communications, procurement and often expert consultants. A breach of any system can set off a chain of events, leading to regulatory disclosures and an investigation, litigation risk and a public relations problem that can severely damage the company's reputation.

New attacks combine technology and social engineering to impact every company employee, vendor and customer. Indeed, commercial contracts are now replete with voluminous and often burdensome terms to review and negotiate. To counsel the corporate client, the in-house attorney must understand not only the meaning of these new requirements, but also whether the company can technically satisfy the specific provisions of such agreements.

Because many companies both utilize and serve as vendors, data security becomes a two-way street. In-house counsel must be engaged in the company's own security as a prerequisite to new business generation, while managing the security risk posed by vendors and other third parties.

Good Housekeeping

As is often the case, in-house counsel is in the best position to coordinate the requisite resources and talent to address the risk. While attacks on security are inevitable and frequent, the corporate attorney can be part of the solution to avoid or mitigate breaches and liability. This begins with creating and manag-

What makes security so unique and difficult to address is the ever-evolving nature of attacks and breaches, creating a moving target that calls for expertise beyond the legal department.

ing a strong internal information security program and a robust vendor management program.

The in-house counsel can lead or be a part of an interdisciplinary security team to establish policies, procedures and incident response/communication protocols. Training of employees has become critical to raise awareness of the myriad traps set by cybercriminals, including spoofed, or fraudulent email requests for information.

The same contract requirements of the company's customers must be considered when dealing with vendors. It is best to have the IT department or outside experts establish formal standards for vendors and an annual audit and review program for significant partners.

Counsel must also develop an understanding of the insurance policies related to cybersecurity, to tailor the right protection under the company's risk management program.

Finally, in-house counsel should play a key role in cyber incident response, where a cyber incident creates significant legal, business or reputational risk for the company.

Rising Expectations

Outside counsel is a key ally in addressing cyber risk and crafting solutions. But there is also an expectation that the law firm will be as compliant with data secu-

rity best practices as the corporation. In a number of industries, that expectation is being codified as regulation. A recent ALM Intelligence Report on law firm cybersecurity noted that more than 70 percent of firms reported increased pressure from clients to improve data security.² This requires a proactive approach and investment in the systems to combat attacks and ensure that the law firm's own data management does not become a security threat to the corporation.

Moreover, the in-house counsel looks to its outside attorney as an advisor to suggest preventative measures and mitigate the impact of an attack. This places a premium on the lawyer to better understand the client's business and potential vulnerabilities. The in-house counsel is looking for more than the statutory requirements that arise when a breach occurs. To navigate the security minefield successfully, both in-house and outside counsel must collaborate and anticipate varying types of events to develop protocols well before an incident takes place.

When such cyber incidents do occur, in-house counsel works with external counsel to manage any crisis, investigate and remediate the incident, and minimize legal, regulatory and other exposures that flow from the incident.

The Impact on Private Lawyers

For private lawyers, data security presents both additional obligations and business opportunities. The obligations are ethical and legal, and they flow from the attorney-client relationship and our own business operations. The opportunities to provide legal services relating to data security grow by the day, and good cybersecurity practices are becoming a business differentiator in all areas of practice.

Competence (Rule 1.1)

Historically, "competence" — the first substantive rule in the *Delaware Lawyers' Rules of Professional Conduct* (Rule 1.1) — referred primarily to the lawyer's substantive knowledge of her area of practice, hence Rule 1.1's expression that "competent representation" requires "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Recent advances in technology, however, have fundamentally changed the way lawyers deliver services to their clients and others. Lawyers now have countless ways to communicate, store and share documents, via smart phones, cloud computing, offsite data storage and various e-discovery-related platforms.

With such conveniences, though, lawyers must educate themselves regarding the benefits and risks of using particular technologies in their practice, as today's lawyer can, with the click of a button, both enhance her relationship with a client or jeopardize the success of an entire matter. Even lawyers resistant or reluctant to using particular technologies must become aware of how technology is affecting their practice area so as to keep up with the lawyers around them and those they supervise.

Confidentiality (Rule 1.6)

A hallmark of our profession, enshrined in Rule 1.6, is that a lawyer "shall

Lawyers and legal organizations should adopt, and periodically review and update, global data security policies tailored to their organization's (and clients') particular needs and risks.

not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry

out the representation, or the disclosure is permitted" under certain exceptional circumstances. Today, that means lawyers make themselves aware of and actively counteract (to the extent possible) the evolving threats to confidentiality stemming from the advances in technology the lawyer takes advantage of, whether concerning transmission or storage of confidential information.

There is no single, correct way to mitigate the evolving security risks. Lawyers and legal organizations should therefore adopt, and periodically review and update, global data security policies tailored to their organization's (and their clients') particular needs and risks.

For further information, the Commission has published its *General Principles of Data Security Planning*, which highlights leading practices in maintaining and improving a lawyer's data security: <http://courts.delaware.gov/declt/blogspot/datasetecuritygeneralprinciples.aspx>

We are pleased to welcome
MATTHEW C. BEARDWOOD



As Managing Director of Marketing
and Client Development

302-633-4040

matt@westovercapital.com

Founded in 1999, Westover Capital Advisors is an independent, privately owned, investment and wealth management firm with a mission to protect and grow our clients' assets. We guide individuals, families and foundations with consistently thoughtful advice and sophisticated investment management to enable them to build and enjoy fulfilling lives for themselves, their families and their charitable interests.



www.westovercapital.com

1013 Centre Road
Wilmington, DE 19805

Communication (Rule 1.4)

Each matter is the client's property, not the lawyer's. Hence, Rule 1.4 — *Communication* — requires, generally, a lawyer promptly to inform the client of "any decision or circumstance" requiring the client's informed consent, reasonably consult with the client regarding how to achieve the client's objectives, keep the client reasonably informed about the status of the matter, and "promptly" comply with reasonable requests for information.

Today, the ubiquity of smart phones, tablets and other mobile devices has profoundly changed the communication expectations of lawyers and their clients: seemingly gone are the days when "out of the office" meant unreachable. As with other ethical obligations, lawyers should assess (and likewise establish expectations) on a client-by-client basis what "prompt" means and what type and frequency of communication regarding a matter is appropriate.

Supervising and managing attorneys should be technology leaders, aware of what technologies the firm and its service providers are using, and what risks those technologies pose.

In addition, lawyers must evaluate what risks certain types of communication (e.g., e-mail, text messaging) may pose and balance against those risks the

needs of each matter (including maintaining confidentiality) and the client's expectations.

Supervision (Rules 5.1, 5.2, 5.3)

It is well established (and now preserved in Rule 5.1) that lawyers with supervisory authority must reasonably "ensure that the other [supervised] lawyer conforms to the *Rules of Professional Conduct*." This principle, under Rules 5.2 and 5.3, also extends to the lawyer's supervision of non-lawyer employees and service providers and, if the supervising attorney possesses managerial authority in the organization, to the organization as a whole.

Today, this means that supervising and managing attorneys should be technology leaders: they must be aware of what technologies the firm (or organization) and its service providers are using, what risks those technologies pose and how they are being or can be mitigated. The Commission has published several *Leading Practices* white papers outlining the

ataxophobia

n. fear of disorder or untidiness

ELIMINATE THE FEAR



Directors Loretta Manning, Marie Holliday & Peter Kennedy

COVER & ROSSITER

CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

It's easy to feel overwhelmed and disorganized, especially by accounting rules and details. Let the experts at Cover & Rossiter apply the latest innovative practices and 75+ years of experience to help you stay organized and compliant, so you can focus on your own priorities.

Great advice. Great people.

www.CoverRossiter.com | (302) 656-6632



@CoverRossiter



/CoverRossiter

appropriate manners in which technology may be used in the practice of law: <http://courts.delaware.gov/declt/practices.aspx>

Liability and Insurance Considerations

Liability for data security breaches under federal and state law is a nascent but quickly growing area. Whether lawyers may incur such liability generally depends on the type of incident and data at issue; contractual obligations and assignment of risk relating to such incidents; satisfaction of disclosure/notification obligations; and the reasonableness of steps taken (1) before the incident to prevent or mitigate it and (2) after the incident to minimize harm, remediate and improve cybersecurity maturity.

For instance, lawyers are subject to data breach notification laws in many states if a “breach” involves covered personally identifiable information. Similarly, lawyers can be “business associates” subject to HIPAA security and breach notification rules.

Lawyers may undertake cybersecurity related obligations and risks pursuant to their client engagement agreements or their vendor contracts. Like other types of businesses, lawyers may be subject to suit by various parties — including, but not limited to, clients — for cyber incidents that impact others.

Insurance coverage for cyber incidents can play an important role in shifting risk. Such coverage is also increasingly required by certain types of clients, providing another differentiator in which lawyers or firms secure certain types of work from particular clients.

Cybersecurity — a Practice Area and a Culture

In light of the explosion in cyber threats and legal issues created by digital technology generally, privacy and data security have emerged as hot, new practice areas for lawyers of all stripes. More than 85 percent of Am Law 200 firms now have a practice group dedicated to privacy and data security.³

Transactional lawyers have brought greater focus to proactive cybersecurity diligence and risk assignment in transactions. Management of third-party cyber risk is of paramount importance. Regula-

**In light of the
explosion in cyber
threats and legal issues
created by digital
technology generally,
privacy and data
security have
emerged as
hot practice areas.**

tory guidance, best practices and formal regulation are keeping regulatory compliance and enforcement lawyers busy. Investigators and litigators have no shortage of cyber incidents to which to respond and resulting civil and criminal litigation to handle as a result of those incidents. The Internet of Things promises to create even greater opportunities for everyone from the patent to the product liability attorneys.

In short, cybersecurity is everywhere, and will grow to touch all types of legal practice. When it comes to cybersecurity, the emergent challenge for lawyers is “to do as we advise.”

Tips for Good Cyber Hygiene and Improved Cybersecurity

Many cyber threats can be reduced by employing good technological hygiene in daily practice. A simple Google search will reveal a wealth of tips about how best to protect your networks, devices and data from the most common threats.

As noted above, the Commission’s website contains leading practices for data security and the use of the most common technological platforms, such as email, cloud services and social media. Below are some top tips to consider:

- Use only approved devices, networks, software and Internet-based services for client services.

- Store sensitive client data only in approved locations/devices.
- Use strong passwords for all accounts and devices (including computers, phones, tablets, printers and Internet of Things devices). Change them frequently. Consider catchphrases that are longer than eight digits and easier to remember than random characters.
- Use a unique password for each website or account, especially sensitive accounts. Consider using password keeper or management software.
- Enable multi-factor authentication for sensitive websites, services and remote access. This form of authentication (widely available on most Internet services, including Facebook, Google, Yahoo, etc.) will require a code, biometric or some other identifier in addition to a password.
- Confirm any wire instructions or requests for sensitive personal or financial information sent by email through phone call or other independent means.
- Encrypt all sensitive email messages and attachments — both in transit and in storage.
- Use secure file-sharing services in lieu of sending sensitive attachments via email.
- Do not click on unknown links or attachments in emails.
- Scan incoming messages, attachments and portable devices for viruses and malicious content.
- Encrypt all devices that contain sensitive data.
- Utilize “lost device” tracking and mobile device management that will enable you to remotely “wipe” a lost or stolen device.
- When purchasing online, check out as a guest whenever possible and use a credit card instead of a debit card.
- Monitor your bank and credit card statements.
- Keep applications, software and operating systems patched and up to date. This includes smartphones and all devices that connect to your firm remotely.
- Back up your data frequently. Keep backups on separate systems that can-

not be reached in the event of a malware (ransomware) attack. Test your ability to revert to backups in the event of a destructive attack.

- Lock your computer when you are away from it. Secure mobile devices (phones, tablets, laptops, etc.) out of visibility within vehicles.
- Do not connect to public Wi-Fi networks.
- Limit access of data to only those individuals who need access and only for as long as they need access.
- Continually educate yourself and your employees about cybersecurity awareness.
- Employ technology or services to monitor network and device usage and periodically conduct external testing and cybersecurity assessments. Implement remediation plans for critical gaps.
- Create a written cyber incident response plan covering each major type of cyber incident you may experience.

Employ technology or services to monitor network and device usage and periodically conduct external testing and cybersecurity assessments.

Implement remediation plans for critical gaps.

Include: team members; incident escalation thresholds; internal and external communications plans; alterna-

tive communications platforms and devices for team members; inventories of users, devices and data; statutory, regulatory and contractual notification obligations; points of contact for all potentially implicated parties; protocols for evidence gathering and preservation; plans for maintaining business operations if data, devices or systems become unavailable.

- Periodically practice your incident response plan with all team members under simulated cyber incident scenarios. Incorporate lessons learned into the plan. ♦

NOTES

1. Given that the ethical rules apply with equal force to all practicing attorneys, it is prudent for the in-house counsel to develop a working knowledge of security and privacy issues, as well as the underlying technology.
2. ALM Intelligence, "Cybersecurity and Law Firms: Defeating Hackers, Winning Clients" October 2016.
3. *See id.*

You May Call Your Best Witness



William A. Santora, CPA
Lori L. Stoughton, CPA

Stacey A. Powell, CPA, CFE, CICA
Robert S. Smith, CPA

Delaware's Premier Litigation Support Team



Santora CPA Group
Right, By Your Side

Call Bill Santora at 302-737-6200



Learning to Cope with Technology Competence Requirements

With lawyers increasingly aware that responsibility for technology and its impacts is not going away, the question is: “What do I need to know?”

The five stages of dealing with grief have been identified as denial, anger, bargaining, depression and acceptance. In 2013 the Delaware Supreme Court amended the Delaware Lawyers’ Rules of Professional Conduct (“DRPC”) to expressly include requirements relating to technology.¹ Those amendments included a requirement under DRPC Rule 1.1 that lawyers “keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...”

Many lawyers grieved over the overt insertion of technology-related requirements into their obligations as lawyers. At first, many engaged in denial: “I don’t need to understand technology for my type of practice.” That was followed by anger: “I’m a lawyer, not a technology consultant!” Next came bargaining: “If I only plan to practice for a few more years, do I really need to learn this technology stuff?” or “If I just hire some technology geeks to deal with these issues, will that satisfy my ethical obligations?” Next came depression: “The practice of law is doomed; lawyers are being replaced by computers.”

Three years out from the adoption of the technology-related amendments to the DRPC, lawyers have now, hopefully, reached the stage of acceptance and recognized that the inclusion of ethical re-

quirements relating to technology is not the apocalypse. Rather, it is just another step in the evolution of the practice of law consistent with the recognition that law follows, not defines, society.

Having reached the stage of acceptance, lawyers begrudgingly seek to understand how they can comply and live with the new technology knowledge obligations. Many lawyers at this stage pose a single, simple request: “Tell me what I need to know in 3,000 words or less.” Well, here is your answer.

1. You need to know how to keep privileged and confidential information privileged and confidential.

Inadvertently disclosing information may be the greatest risk posed by lawyers’ use of technology. DRPC Rule 1.6 requires reasonable efforts to prevent

inadvertent or unauthorized disclosure of information relating to the representation of a client. Comment 19 to Rule 1.6 requires a lawyer to make reasonable efforts to prevent disclosure.

We addressed the basics of this topic in an earlier article and will not repeat that discussion here.² We only note the multiple venues that technology provides for inadvertent disclosures which include: (a) misaddressed emails; (b) lost or stolen mobile devices or use of such devices in public where information can be seen or overheard by others; (c) use of simplistic passwords that can be easily determined; (d) use of insecure public Wi-Fi systems; (e) legitimate-looking but fraudulent emails requesting information or money, including emails containing attachments or links that if opened provide the sender with access to your computer system; (f) utilizing cloud-based systems that are not adequately secure or private; (g) deliberate cyber-attacks on your computer system by third parties attempting to gain access to your computers, which are often made easier by lawyers with insufficient security on their computers and networks; (h) discussing client matters or cases on social media; (i) inadvertently disclosing information intended to be withheld or that the lawyer did not even realize was there (*i.e.* metadata) when transmitting or producing electronic documents and records both in general correspondence and discovery.

More detail on many of these topics is available at the “Leading Practices” section of the Commission web site: <http://courts.delaware.gov/declt/practices.aspx>

2. You need to know what fraudulent emails and phishing scams look like and that law firms are regularly targeted.

This relates to No. 1 above but bears special mention. According to a March 2016 FBI press release, from October 2013 through February 2016, e-mail-related schemes targeting businesses that regularly perform wire transfer payments have resulted in \$2.3 billion in losses.³

Often in such schemes, the criminals conduct research to determine who at a company manages money. They then

Advising clients may require that lawyers consider and discuss the client’s social media practices and how they might affect their legal rights in matters the lawyer is handling.

send an email to such person that appears to come from another person within the target organization or from a client or customer.

Several of these types of scams have occurred in Delaware recently. In one, a Delaware real estate firm received an email directing that proceeds from a real estate settlement scheduled for that same day be sent to a different (and fraudulent) bank account. That led to the “alert” posted on the Commission web site.⁴

In a second, the office manager of a Delaware firm received an email that claimed to be from one of the senior partners at that firm instructing that an immediate wire transfer of money be made. The manager attempted to follow up with the partner and determined the email was fraudulent before any transfer was made.

The point here is that fraudulent emails no longer involve just requests from a stranger in Nigeria asking for help to claim millions of dollars left to them by a deceased relative or seeking legal representation of a matter “in your jurisdiction.” They often appear to be legitimate emails from someone the lawyer knows and they are occurring in Delaware.

To see what various iterations of fraudulent emails look like, visit the FBI Internet Crime Complaint Center at <https://www.ic3.gov/media/default.aspx>

3. You need to understand how social media might help or hurt your client, and how to preserve and obtain information from social media without violating professional obligations.

Social media generally refers to web sites that serve as virtual communities, in that they allow people to share information, ideas and generally to socialize through an on-line site. Better-known examples include Facebook, MySpace and GooglePlus.

Competence in advising clients may *require* that lawyers consider and discuss the client’s social media practices and how they might affect their legal rights in matters the lawyer is handling. Lawyers must also inquire regarding, and know how to preserve, information from social media that a client creates or controls.

Lawyers must understand how to gather information from others using social media without violating the rules that govern lawyers’ communications with other parties. For example, sending a “friend” request through Facebook or similar social networking site (even though the recipient accepts it) may constitute a communication that could violate various restrictions contained in DRPR Rules 4.1 through 4.3.

Lawyers must understand that clients sometimes view their social media pages as “private” communications and warn them about the risk of waiving the attorney-client privilege if they discuss their communications with the lawyer on social media.

And lawyers must understand how to make sure that information gathered through social media is admissible at trial (or how to challenge its admissibility) and the ways that social media can affect the outcome of jury trials.

For more information, see the Social Media Leading Practices page on the Commission web site: <http://courts.delaware.gov/declt/social.aspx>

In case you haven’t noticed, social media is everywhere. As of September 30, 2016, Facebook had 1.79 billion monthly active users. Photo-sharing app Instagram takes second place with 500 million monthly users (up from 400 million in 2015). Twitter has 370 million active users, including the president.

Messaging app Snapchat boasts 150 million users after just four years since its release.

The ubiquity of social media poses new security risks and challenges. The risks are serious and they are real. Delaware's Rules of Professional Conduct require all lawyers to be competent in the practice of law, including in their understanding the risks and benefits of technology.⁵ The Rules also require that we ensure the compliance of the lawyers and staff for whom we are responsible.⁶

Thus, all lawyers — not just those who are active users of social media — should be aware of the risks and take steps to prevent them.

Denial Is Not a Strategy

In the case of cyber security, ignorance is a recipe for disaster. To put blind faith in social-media companies to protect you and your data would be foolish, if not reckless. The most common social-media attacks are directed attacks on individuals. For example, in 2015, Facebook scams were the most common method of distributing malware (software designed to infiltrate computers with the user's consent).

In 2012, a hacker stole 6.5 million encrypted passwords from LinkedIn and posted them to a Russian crime forum. In 2016, a Russian hacker began selling 117 million of the stolen email and password combinations. Following that event, Facebook CEO Mark Zuckerberg and Twitter founder Jack Dorsey had their social-media accounts hacked. If social-media CEOs are susceptible to cyber-attacks via social media, so, too, are we.

Social media is particularly susceptible to the following methods of cyber-attacks:

Social Engineering

Social engineering relies on human trust instead of technology. Social-media sites can provide an attacker with significant amounts of personal details, such as work and home addresses, phone numbers and birth dates, just to name a few.

Attackers can use publicly available information to learn more about their victim and build trust by, for example,

Consider restricting access to social-media sites on your firm's computers. It may not be popular but it is far safer than allowing individuals to access potentially harmful software or links that can wreak havoc on your firm's operations.

expressing interest in the victim's areas of interest.

Attackers also can gain access by friending members of the victim's social networks, which causes the victim to assume the attacker to be a credible associate.

Spear Phishing

Spear phishing involves an attempt to trick the victim into clicking a link or opening a document. Spear phishers send malware through social-media sites, such as Facebook's Messenger, in order to avoid the traditional security controls frequently implemented on email systems.

Prevention Is Possible

As overwhelming as it may seem, there are steps you can take to avoid security breaches through social media:

Inform and Educate

Consider implementing a social-media policy for employees in your firm. The National Labor Relations Board, the agency that enforces the National Labor Relations Act, which applies to employers, including law firms, takes a very narrow view of acceptable social-media policies, so it's wise to consult with expe-

rienced employment counsel when drafting such a policy.

If a policy doesn't feel like the right fit, consider as an alternative social-media guidelines — suggestions for appropriate social-media use — that can be published to your employees.

Regardless of whether you elect to implement a policy or create a set of guidelines, and even if you decide to do neither, you should educate the lawyers and staff in your office about the risks of social media. If nothing else, start a dialogue about those risks and about ways those risks can be avoided. A conversation costs nothing but can plant the seed of awareness, which often is key in avoiding social-media missteps.

You can initiate the conversation in any number of ways. Consider raising it at a staff meeting, or hosting a lunch-and-learn and ask attendees to bring a news story involving a social-media gaffe. Circulate such stories yourself. It needn't be complicated or expensive or formal, as long as it builds awareness.

Limit Access

Consider restricting access to social-media sites on your firm's computers. It may not be the most popular move but it is far safer than allowing individuals to access potentially harmful software or dangerous links that can wreak havoc on your firm's operations.

If you need additional motivation, consider your ethical obligation to preserve your client's confidential information. Failure to take reasonable steps to avoid unauthorized access to privileged information could violate your duty of confidentiality.⁷

A common argument against limiting access is that employees will just access such sites via their phones. And this is likely true — it would be foolish to think that employees won't check Facebook during the workday merely because they are unable to do so via their desktop computers. However, by limiting access, you can mitigate the risk that your system will be infiltrated by malware or other unwanted and dangerous applications.

4. You need to understand how the use of technology in the courtroom might increase or decrease the chances of success for your client —

and when the use of such technology may pose ethical concerns.

Some reports suggest that jurors have been influenced by the “CSI Effect” and now expect to see technology and technological evidence in the courtroom.⁸ Thus, lawyers need to understand how the use of technology to establish or present evidence may be perceived by and influence a jury.

Lawyers must consider how digital evidence that is presented at trial will be preserved as part of the trial record because it can pose unique problems. Most basically, lawyers need to know how to use the technology that will be used at trial.

For more detailed information, see the Courtroom Technology Leading Practices section of the Commission web site.⁹

5. You need to know how to avoid spoliation of electronic evidence by your client and where and how to obtain discovery of electronic information from other parties.

Electronically stored information, or “ESI,” has changed the nature and volume of discovery significantly. Email, voice mail, text messages and social media sites have become the sources of much significant evidence. Because such information exists electronically on computers and networks that are numerous and constantly changing, lawyers need to be aware of the risk that information that exists when a case begins may be destroyed or altered simply by normal everyday use of the computers and other devices on which such information is stored.

Thus, lawyers should at the outset of every litigation-related matter identify such information and take steps to avoid its destruction or modification. Lawyers must be familiar enough with the various forms of ESI (which includes some “hidden” information such as metadata) to help their clients know where to look for it, and to verify that opposing parties have taken sufficient steps to preserve and identify such information.

For more detailed information, see the eDiscovery Best Practices section of the Commission web site.¹⁰

Last year, California issued a formal opinion regarding an attorney’s ethical

Because digital evidence (such as spreadsheets) can be manipulated in ways so as to present the stored information in various forms, the line between whether digital evidence is real or demonstrative can be blurred.

duties that is fairly comprehensive and provides a good overview of many ethical issues that surround eDiscovery.¹¹

Email, text messages and social media sites are often gold mines of significant evidence. Lawyers who do not protect and mine evidence from these sites may not be competently representing their clients and may be exposing their clients and themselves to significant sanctions, as already have been imposed by many courts.

For more detailed information see the View from the Bench Leading Practices section of the Commission Web Site.¹²

Because much evidence is now digital, lawyers need to understand that there are unique issues involved with authenticating digital evidence. Lawyers must consider whether digital information being offered as evidence is real evidence or demonstrative evidence because the rules of admissibility differ. Because digital evidence (such as spreadsheets) can be manipulated in ways so as to present the stored information in various forms, the line between whether digital evidence is real or demonstrative can be blurred.

So, We Lied

Ok, we admit that we have not provided to you everything you need to know to satisfy your obligations to be competent with respect to technology in your practice. Instead, we have provided you with a checklist of the main areas that lawyers should at least be aware of to avoid technology-related ethical problems, and we have provided you some sources to explore those topics further. We did do that in fewer than 3,000 words, so at least that part was true.

In particular, we encourage Delaware lawyers to take advantage of the resources offered by the Commission. The Commission’s web site has a help desk feature where you can submit questions and thereby avail yourself of the collective knowledge of the Commission’s members.

We hope that you have reached the stage of acceptance. If you are not there quite yet, we are sure that it will not be much longer. ♦

NOTES

1. <http://courts.delaware.gov/rules/pdf/DLR-PC-LN.pdf#search=professional%20conduct>.
2. See Bruce Jameson, *Technology Competence for Lawyers: Not an Oxymoron*, 32 Del. Law, no. 3, Fall 2014, at 16.
3. FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals: <https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals>.
4. <http://courts.delaware.gov/declt/alert.aspx>.
5. See Del. Lawyers’ R. Prof’l Conduct 1.1, cmt. [8].
6. See Del. Lawyers’ R. Prof’l Conduct 5.1 and 5.3.
7. See Del. Lawyers’ R. Prof’l Conduct 1.6.
8. See e.g. ABA Trial Evidence Committee, Managing the CSI Effect in Jurors, <https://apps.americanbar.org/litigation/committees/trialevidence/articles/winterspring2012-0512-csi-effect-jurors.html>.
9. <http://courts.delaware.gov/declt/courtroom.aspx>.
10. <http://courts.delaware.gov/declt/ediscov-ery.aspx>.
11. [http://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202015-193%20%5B11-0004%5D%20\(06-30-15\)%20-%20FINALL.pdf](http://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINALL.pdf).
12. <http://courts.delaware.gov/declt/blogspot/spoliationofevidence.aspx>.

FEATURE

The eDiscovery
Leading Practice Group

Cybersecurity Implications in e-Discovery

Clients demand that
attorneys and their
vendors protect —
and at litigation's
end, return, destroy or
secure — data
collected in discovery.

*"Law firms are the soft underbelly of corporate cybersecurity."*¹

According to the FBI,² the current reality is that many law firms are the subjects of hackers' ire. What was once secure in a client's possession may now be vulnerable in that client's attorney's files. With an increasing concern regarding the confidentiality and security of electronically stored information ("ESI") collected in discovery, there are a variety of factors to consider.

From what clients are demanding of their counsel to considerations when retaining an electronic discovery vendor to issues arising when receiving and sharing ESI with opposing counsel and the Courts, cybersecurity is no longer the singular concern of the owner of the ESI. Equally as important are issues facing others who possess this data — notably lawyers.

What Clients are Demanding

According to Rule 1.6(a) of the Delaware Lawyers Rules of Professional Conduct, "A lawyer shall not reveal information relating to the representation of a client"

While no Delaware cases have yet applied this standard to situations where an attorney was in possession of confidential information that was ultimately compromised, it appears that clients are not sitting by idly. Rather, before they hand

over their highly confidential information, clients are increasingly demanding high levels of security of their data from their lawyers.

For example, Delaware's own Bank of America has announced that it was conducting a security audit of its law firms. According to Assistant General Counsel Richard Borden, Bank of America is "one of the largest targets in the world" for cyberattacks and law firms are "considered one of the biggest vectors that the hackers, or others, are going to go at to try to get to our information."³

From Bank of America's perspective, Borden said, the Office of the Comptroller of the Currency has focused on law firms; "[t]hey are coming down on us about security at law firms. So we have no choice but to check the information security and to audit — to actually audit — the information security of our law firms

that have confidential information. We spend a lot of money and use a lot of law firms, so this is casting a very wide net.”⁴

While it may be easy to distinguish Bank of America and other specially regulated entities from your client base, the data suggests otherwise. Rather, firms are reacting to client concerns.

Among the measures being taken are firms seeking “ISO 27001” cybersecurity certification. This form of certification is intended to help organizations, including law firms, “manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.”⁵

Why are firms seeking such certifications? The reasons:

- Approximately 71 percent of respondents have clients who request this type of certification;
- Approximately 56 percent are seeking a competitive advantage over other firms;
- Approximately 33 percent believe such certification is necessary for maintaining existing clients or getting new business.⁶

Since clients naturally are interested in how secure their data is, attorneys need to consider what steps they can take to keep that information secure and meet their client’s expectations.

Security Considerations and Vendors

Using an eDiscovery vendor to collect, process, review and produce documents in the course of litigation, or for a government investigation, has been the norm for a majority of law firms, both large and small, for nearly two decades. The thought that these vendors may present a threat to the security of clients’ data only recently has been a subject of discussion.

As we know, an attorney’s responsibility to keep clients’ information confidential extends not only to the firm she is affiliated with, but also to the agents that attorney uses to manipulate and store data. Ensuring your eDiscovery vendor is capable of adequately securing client data requires knowledgeable inquiry, not just of their technological security, but also their physical security and their protocols for providing the most secure environment possible.

Ensuring your eDiscovery vendor is capable of adequately securing client data requires knowledgeable inquiry of their technological security, their physical security and their protocols.

Questions you should ask your eDiscovery vendor before you hire them include: What has their investment been in recent years to prevent invasion by hackers into their environment? What methods of encryption and transmission protection do they employ, and have those been tested and audited recently? Does the vendor perform background checks of its employees and contractors and do they have different levels of physical security for different levels of employees?

Answers may vary from very specific responses including security certifications such as ISO 27001 or Federal Information Security Management Act of 2002 (FISMA) Authorization to Operate (ATO), to vague references of not being breached in the past.

When hiring an eDiscovery vendor, it is also a good practice to have either your firm IT security specialist or a trusted third party conduct a security audit of the vendor to confirm that the vendor’s technology and protocols regarding cybersecurity are sufficient such that you can satisfy your ethical obligations.

Security Considerations and Data Transmission

Moving data and producing data during the course of litigation carries with it another set of specialized risks that in the past have not been considered very often. But now, in a world where hackers can ac-

cess your data from anywhere, the competent lawyer must be on guard against even the most mundane circumstances.

Producing electronic documents during the course of litigation, once a simple clerical task, now must be designed with the highest security in mind. What if that flash drive or DVD containing documents that were produced in litigation is lost in the mail or even stolen? Encryption software is readily available which would make the media nearly impossible to access and should be used on *any* device containing client information leaving a lawyer’s possession.

A protective order is another tool that should be employed by parties in litigation to ensure that both the recipient of the data and the court are capable of maintaining confidential information in an appropriately secure manner. Drafters of protective orders have contemplated filing confidential documents under seal for many years; in fact this is a common practice. However, lawyers often overlook the ability to define *how* the receiving party will secure information, as well as instructions on maintaining confidentiality when sharing with third parties, experts and the court.

Lawyers should consider including language in the protective order that would require the receiving party to use the same means of securing the produced information as they would use to secure their own clients’ information. An effective protective order should outline the steps to take when sharing confidential information with experts, such as providing access to a closed workspace, requiring background checks for employees, contractors and agents, and encrypting and password protecting all storage devices and transmissions, both electronic and physical.

When the Case is Over

You won or you lost, but what do you do with all of the confidential information now that the case is over?

First, was there a protective order or other order governing the protection of confidential information entered in the case? If not, then confer with opposing counsel and your client to establish an agreed-upon protocol for returning or destroying the confidential information exchanged in the case.

If the parties agree that certain confidential information or categories of documents (emails, correspondence, etc.) may be retained by counsel, then you should determine what protocols will govern ongoing protection of the retained confidential information.

It is important to note that an attorney's duty under Rule 1.6(c) to make reasonable efforts to prevent inadvertent or unauthorized disclosure of a client's information continues not only after a case has ended, but after the lawyer-client relationship has ended, as well. This applies to third-party vendors that may have been retained to assist with the representation, such as e-discovery vendors. *See* Rule 5.3.

Accordingly, it is incumbent upon a lawyer to be as involved and protective during the wrap-up process as he or she was in handling the litigation itself.

Second, if there is a protective order, what does it say? Document return or destruction provisions are common in protective orders. The specific terms that

It is incumbent upon a lawyer to be as involved and protective during the wrap-up process as he or she was in handling the litigation itself.

may apply to a given case, however, may vary widely.

Generally, protective orders provide for a set time period after the case is concluded for the parties to comply with the return or destruction provisions. Such provisions usually permit counsel to re-

tain at least one copy of certain categories of documents such as pleadings, motions and briefs, depositions transcripts, correspondence, expert reports, written discovery responses, trial transcripts and hearing or trial exhibits.

Any retained data typically continues to be governed by the protective order even after the case is over. Some protective orders go one step further and specifically impose upon each party an affirmative obligation to request the return or destruction from experts, advisors and/or vendors.

The most variance between return or destruction provisions relates to correspondence. In that regard, some protective orders permit counsel to retain correspondence generally. Other protective orders may have no such carve-out for correspondence, thereby requiring complete eradication of the other side's confidential information from all correspondence files (emails, voicemails, text messages, backups and archives).

Once the terms of the specific return

Over 50 Years of Superior Customer Service

IT Network Solutions • Managed Network Services • Multifunction Copiers & Printers



Accredited by
BBB of Delaware

Hilyard's
INC.
Business Solutions
Network Solutions & Document Management

1.800.247.2201



Ask about our Bar Association Discounts

Dover, DE | Salisbury, MD | Wilmington, DE | www.hilyards.com

Canon KIP LEXMARK SHARP

or destruction provision are clear, then compliance can begin.

Third, where are the hiding places for confidential information? Paper copies of confidential information are fairly easy to find and collect. Electronic documents should be easy to find as well, but with the advances in data security and technology management it can take some skill to find all of the places in which confidential information can be hiding.

Likely areas for electronic storage of confidential information are personal drives, email folders, personal mobile devices or laptops, shared drives and production databases. Other locations to consider are voicemail boxes, intranet files, internet files, cloud-based storage or file-sharing sites and physical media (such as flash drives and CDs).

In addition, just as the e-discovery process may have required review of client back-ups or archives, confidential information could be sitting on the firm's back-ups or archives.

Fourth, remember the vendors! During the course of the litigation, confidential information may have found its way to a document management company or e-discovery vendor, to a jury data analyst company or to some other professional services company. It is likely that such companies are already aware of the protective order in the case and may even have signed an undertaking agreeing to treat the data they receive in accordance with its terms.

Now that the case is over, however, a best practice for counsel is to send a notice that the case is over to any companies that provided assistance during the case and may have received confidential information. This notice should be provided regardless of whether the confidential information was from one side or the other in the case.

The important point is to provide notice and a reminder regarding the terms of the protective order or instructions regarding how to treat the confidential

information going forward.

Conclusion

While we may not have previously considered the security of data received and produced in discovery, the security implications are no different than those for other forms of data. In order to properly serve — and attract — clients, attorneys need to be mindful of how that data is protected. ♦

NOTES

1. See <http://www.ediscoverylawtoday.com/2014/05/the-importance-of-data-security-in-ediscovery>.
2. *Id.*
3. See http://www.americanbar.org/publications/law_practice_magazine/2013/november-december/hot-buttons.html.
4. *Id.*
5. See <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.
6. <http://www.corpcounsel.com/id=1202766430631/Legals-Business-Necessity-Client-Demand-Spurs-ISO-27001-Cybersecurity-Certification?slreturn=20161020184337>.

GET READY FOR A WINNING COMBINATION.

Mailboxes • Packing & Shipping • Printing

Check out everything we do at The UPS Store®. We offer services that make life easier and help keep businesses running smoothly.

4023 Kennett Pike
Wilmington, DE 19807
302-429-9780
store1391@theupsstore.com
www.theupsstorelocal/1391.com

Hours:

Mon-Fri 7:30 a.m.-7:00 p.m.
Sat 9:00 a.m.-4:00 p.m.
Sun Closed



The UPS Store®



WE ♥ LOGISTICS™



Email Technology, Security and Privacy

Email threats are ubiquitous, from links to malicious software to the vulnerability of sensitive client information.

Most people think the purpose of email security is to prevent spam from coming into the network and to stop viruses from infiltrating the system. Those types of threats are becoming more sophisticated every day.

Email security, however, is not something that only IT staff have to concern themselves with. Increasingly lawyers need to think about the safety of their clients' data within their firms' email and servers. The definition of "reasonableness" under Rule 1.6(c) will shift as more tools arrive that make file transfer and sharing easier and more secure.

There is no greater threat to clients' data than through law firms' email systems. Law firms, large and small, must consider the kind of data that is being stored in the mailbox, where it is being stored and how best to safeguard it.

Over the past decade, it has become all too common to use email for more than just communicating. Users now often store, organize and archive client records in email (such as Outlook), which is very user friendly. Obviously, this leads to a proliferation of client data stored on email systems.

Some client data may be stored in email that dates back five, 10 or 15 years, far too long. There are various methods that can address this potential issue; for example, a

policy may be implemented to automatically remove email after a certain length of time.

Law firms are increasingly becoming the targets of hackers because of client-sensitive data, such as Intellectual Property and corporate information relating to such things as mergers and acquisitions. Threat actors also target clients' personal data such as Personally Identifiable Information (PII) and Personal Health Information (PHI). The average cost of a data breach in 2016 was \$4 million.¹ Protection of clients' data begins with email.

Receiving Email

The biggest nuisance when receiving email is dealing with the massive amount of spam email. Spam is generally not malicious but can flood an inbox with unwanted email, reducing productivity and increasing the load on the firm's email server. Spam filters can eliminate most unwanted spam and there are cloud solutions that filter for spam email before it reaches the email server.

There are potential downsides to aggressively filtering spam, however. False

positives can lead to missed client email. Spam email must be reviewed by the lawyer or other professional for valid messages.

When the Democratic National Committee was hacked in 2016, one envisioned sophisticated hacking technologies that penetrated the DNC network defenses. In reality, the hack was the result of a phishing attack, where a DNC official clicked on a link and entered his password.²

Phishing attacks have become more sophisticated as hackers learn to penetrate spam filters and become more targeted in their attacks. Targeted (or Spear Phishing) attacks focus on specific high-profile users within organizations. Whaling, or so-called “CEO Attacks” attempt to spoof CEO-level executives to send email to accounting staff in an attempt to wire funds. This has happened within the Delaware legal community in 2016.

Accounting staffs should be trained to be wary of any email coming from a managing partner and proper checks and balances should be implemented to verify all wire transfers. Links inside of unsolicited messages should never be clicked.

Even if one is sure the email is legitimate, a good practice is to open the internet browser and go directly to the website, instead of clicking on the link in the email. Consider using services that offer URL Protection, which can modify links inside of an email and verify the safety of the website if the link is followed.

In addition to stealing user credentials, clicking on links in phishing emails can also introduce malicious viruses such as keyloggers, cryptolockers and back doors. Keyloggers capture all of a user’s key strokes, usually with the goal of stealing your online banking credentials. Back doors install software that allow the attacker to connect to the targeted network at any time. Cryptolockers or ransomware are attacks that can encrypt files on the local hard drive, as well as any network drives. Once the files are encrypted, the attacker demands payment (usually in the form of bitcoin) to unencrypt the files.

Because of attacks like ransomware, users should only have rights to those network drives and folders necessary for their practice. Furthermore, client records should never be saved on the local hard drive as these drives are usually not backed up.

Once sent, an email can live forever. Files that contain information such as social security numbers, medical information, credit card information or bank account information should never be sent via email.

Viruses such as the above can also come in the form of attachments. While virus filters are a good first line of defense at stopping malicious attachments from reaching email, hackers are becoming more sophisticated in penetrating the filtering defense. For example, macro viruses, which are coded instructions inside of Word and Excel files, can go undetected in virus filters. If macros are not disabled, macro viruses can execute by opening the file. Malicious links can also be found in PDF files.

Because of these types of hidden viruses, services are available that can “sandbox” email attachments. Sandbox services open the attachment in a safe environment and can detect whether the file is malicious before it reaches the inbox. Furthermore, certain file extensions should always be blocked from email such as: .exe .js .jse .vbs .vbe .iso .hta and .wsf.

Sending Email

Security and privacy need to be a concern when sending email, as well. Email can be intercepted by third parties. Once sent, the email resides in the recipient’s mailbox where the original sender has no control. Security and privacy concerns are paramount in consumer, web-based email such as Gmail. Increasingly, lawyers need to be aware of client data inside of email and email attachments, especially where PII and PHI are present.

In order to protect against email being intercepted in transit, email transmission can be encrypted. Most email servers have the ability to send and receive email using Transport Layer Security (TLS) Email Encryption. TLS is typically set up to send using encryption, meaning that if the receiving server can accept TLS, it will be sent using TLS; otherwise the email will be sent in clear text. TLS can also be set up to force the use of TLS between the email server and the client’s email server. Many financial clients require the use of TLS.

Remember that TLS only encrypts the email transmission. Once the email is received, the email is not encrypted in the recipient’s mailbox or in the sender’s sent items folder.

Once sent, an email can live forever, depending on the email systems and third-party services involved. For this reason, email and attachments that may contain PII or PHI deserve special attention. Files that contain information such as social security numbers, medical information, credit card information or bank account information should never be sent via email. Nor should such information be transmitted as part of the body of an email.

Users need to be trained to identify PII and PHI and be aware that the document may require special handling. When transmitting protected information, consider using cloud-based file sharing services. Several file-sharing services exist that can offer secure file sharing and can facilitate secure file transmission via email.

Storing Email

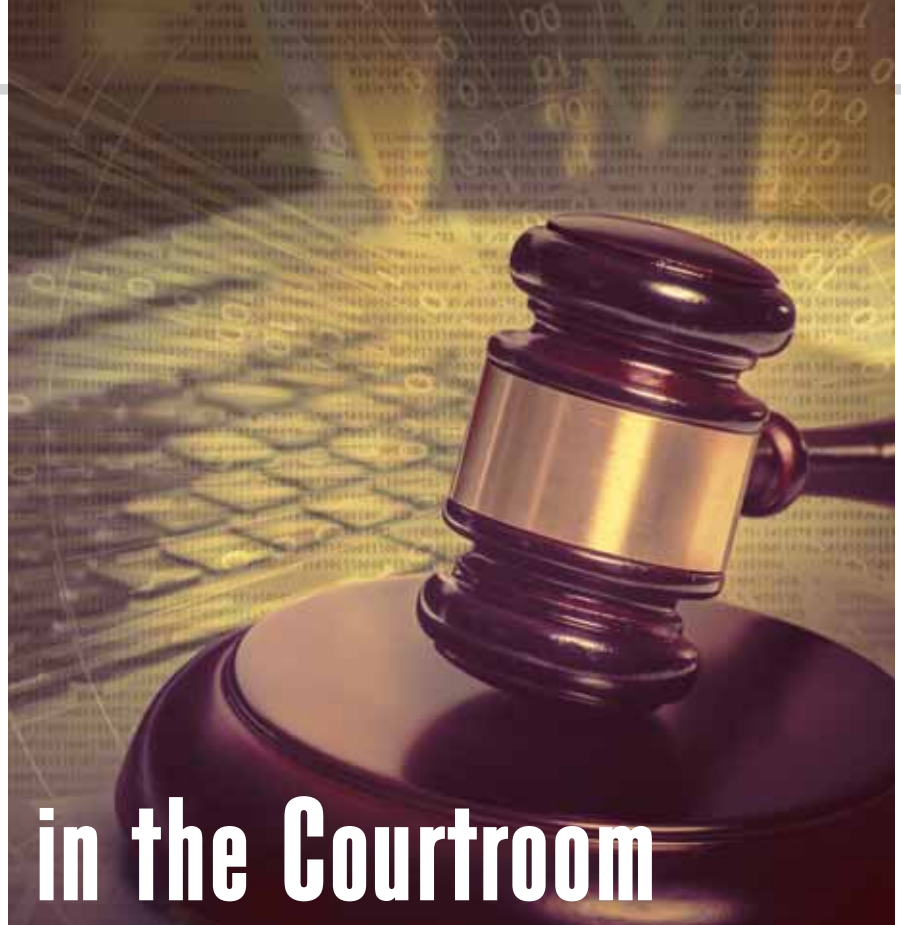
A discussion of email security and privacy must also include the storage of email, not only in one user’s mailbox, but also in the entire firm email database. A mailbox is only as secure as that user’s login credentials. If a password is compromised the entire mailbox will be breached.

Limiting the amount of email stored in mailboxes will limit your exposure in the event of a breach. If client email is stored in a mailbox it should be organized into folders that identify the client matter. If possible, move a client email to a secure document management system.

*See **Email Security**
continued on page 27*

FEATURE

The Courtroom Technology
Leading Practice Group



Wi-Fi in the Courtroom

Understand the technological capabilities of the courts where you will practice to ensure effective presentations and the security of client data.

The practice of law continues to evolve from analog to digital — from paper files and tangible evidence to electronic files and digital reenactments. Digital repositories are a mainstay of the legal profession.

Pleadings are researched, drafted and filed electronically. Bankers Boxes of paper files are being replaced with thumb drives and cloud-based storage. In most cases, voluminous pre-trial discovery is managed and provided electronically. Rather than binders and briefcases, many attorneys now rely on computers and tablets to advocate on behalf of their clients.

These tools allow Delaware lawyers to work more efficiently, effectively and conveniently. With the mobility and adaptability of today's technology, attorneys are bringing these tools into the courtroom.

These are the facts of legal practice. To succeed in the future, attorneys must use appropriate tools and have a solid understanding of the risks and benefits to professionally use technology in the courtroom. While wireless access abounds, the use of this technology in the courtroom environment presents unique considerations.¹

Technology in the Courtroom

Technology is used in court during trials and hearings to better present ideas and arguments. Attorneys must be aware of

the technological capabilities and limitations in the courtroom. Most courtrooms in Delaware's state and federal courts provide basic "wired" connections; however, as the rooms are upgraded, wireless capabilities are being enhanced. Moreover, advocates with some technical proficiency may choose to build a temporary network to support their presentation.

Of course, the Delaware Lawyers Rules of Professional Conduct strongly encourage the use of technology in the courtroom. See Del. Lawyers' R. Prof'l Conduct 1.1. (Competence). In addition to using technology to present a case, attorneys may also use available networks to access files while in court. With hours spent in the courtroom environment, a reliable network is essential for the productivity of today's litigators.

Security Concerns

Confidentiality, privacy and the integrity of one's work product are concerns inherent with any use of technology. Courtroom data connections present special challenges for attorneys.

Connecting your device to a network may expose information on your device to another user on the same connection. Ignorance of these security issues raises special ethical concerns for attorneys. An attorney has an obligation to protect a client's confidential information from "inadvertent or unauthorized disclosure."² Further, attorneys must take "reasonable precautions" to ensure that communications containing confidential client information are secure and do not "come into the hands of unintended recipients."³

While the rule "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy[,] [s]pecial circumstances, however, may warrant special precautions."⁴ A lawyer should consider factors such as "the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement"⁵ when determining whether special precautions are required.

However, there are solutions to allow secure, convenient and connected access for attorneys. One solution is a dedicated wireless network. These networks can require strong password protection and restrict access to attorneys and their staff. While such a system may not be able to track individual attorney actions on the network, it would reasonably restrict access to the network from the general public.

Another alternative is to create a network only available to the attorneys who have matters in the particular courtroom. Rather than have a static password available to all attorneys at all times, the court could change it on a case-by-case basis. This would allow the court to keep access open to the attorneys for the matter presently being heard until the matter concludes.

While this more restrictive policy would afford greater security, it would be to the detriment of attorneys in the courthouse who may need internet access, but do not have an immediate pending case.

Many courts have already set-up wireless systems for use in courtrooms. Presently, the U.S. District Court for the Northern District of California will not allow attorneys to use anything but wireless connections.⁶ The Florida courts have

There are a number of ways to create secure internet access for attorneys in the courthouse. Ultimately, the solution must be able to accommodate all the attorneys who require access, while simultaneously keeping information safe and secure.

begun such use in the 9th and 12th Judicial Districts. Moreover, in the United Kingdom, the judicial system began "rolling out" digital courtrooms in 2013, including wireless use in 500 courtrooms.⁷

There are a number of ways to create secure internet access for attorneys in the courthouse. Ultimately, the solution must be able to accommodate all the attorneys who require access, while simultaneously keeping information safe and secure.

Reliability Concerns

Another concern is the reliability of the connection. Attorneys may depend on the network at critical times, such as giving an opening or closing argument. Therefore, a wireless network must be fast enough to accommodate the attorney's needs and be able to support multiple users. To understand what is required for such a network, it is helpful to have a basic understanding of Wi-Fi and the factors that affect its adequacy.

Wi-Fi is the use of radio waves to transmit digital information. There are numerous factors that determine how quickly the information is transmitted, such as bandwidth, speed, gigahertz, latency, ping and many other technical terms you may hear

from a Verizon commercial or your local Best Buy salesperson. A brief explanation of some of the factors that affect a wireless connection is helpful to determine what is required.

Bandwidth and speed are terms that seem to be used interchangeably. However, they are two separate cogs in the proverbial Wi-Fi machine. Bandwidth refers to the capacity of a network, or how much information can travel across the particular network. Speed refers to rate of speed of the information traveling over the network.

Imagine a wireless network as a two-lane highway over which data is being carried by cars. Speed refers to how quickly those cars can travel to carry the data. Bandwidth refers to how many lanes are available on the highway.

If the speed limit is 65 miles per hour, that is the fastest the car can travel. However, if there are many other cars on the road, the congested highway may slow traffic. Add enough cars, and eventually a traffic jam develops. However, if we add more lanes, going from two to six, for example, it allows the cars to reach their maximum speed because there is less congestion.

Both bandwidth and speed are important. Even with the fastest speed available, if too many users are on the network, that speed can never be reached due to congestion, resulting in a slow or sluggish connection. Likewise, having a large bandwidth will allow a larger number of users, but if the information does not move quickly enough, the connection will again be slow.

Therefore, a proposed attorney network would have to consider how many people would be using it at a given time, and how much information those users would be transmitting over the network.

Wireless Hardware Connections

Along with the internet, there are other wireless capabilities that could be useful in the courtroom. Wireless connections of computers and laptops to courtroom projectors or video monitors would eliminate, or at least substantially reduce, the number of wires required for using technology in the courtroom.

Not only would this reduce any clutter from the installation of wires, but it would also reduce installation costs because little or no construction is needed.⁸

One method of wireless hardware con-

nections is a wireless High-Definition Multimedia Interface (HDMI) connection. The benefit of HDMI, wired or not, is that both audio and video can be transmitted over one connection. It does not matter if you want to display a video, sound, picture or text, it can all be done via a single HDMI connection.

A wireless HDMI system consists of a transmitter and responder. The transmitter is connected to the laptop or tablet and the responder to a display, such as a monitor. An attorney can then wirelessly display whatever is on his or her computer to the monitor.

With a wireless HDMI connection, the attorney would not be limited in where he wanted to connect his device. It could be connected at the table or lectern. Also, because it does not rely on Wi-Fi, there is more reliability in the connection. The system can be installed without running any wire or cables from the computer to this display. There are, however, potential drawbacks.

One issue is that communication errors can occur between the transmitter and responder. Some systems require a direct line of sight, meaning there cannot be any obstructions between the devices. Additionally, the connection would not be as reliable as a wired one.

Compatibility could also be an issue. Normally, one only has to plug in the corresponding units for the system to work. Technology, however, is not always so user friendly. Some systems may not work reliably with all types of devices or computers. Further, some popular devices, such as iPads, do not have HDMI ports and require adapters for HDMI connections.

An alternative for wireless connections to displays and monitors are Wi-Fi-connected mirroring devices, such as Google Chromecast or Airtame. These devices are installed into the display, such as a TV, and then connected to a Wi-Fi network. Once connected, any other supported device, such as a laptop, iPad or even a smartphone, can connect to the same Wi-Fi network (or via Bluetooth) and mirror what is on their device to the display.

One advantage of mirroring devices is that, unlike wireless HDMI, nothing

In this digital age, technology is becoming more a necessity than a novelty. The sooner it is embraced, albeit with caution and care, the sooner the legal community will reap its rewards.

needs to be physically connected to the computer or tablet. All that is needed is the installation of the device's software. This avoids needing multiple transmitters, or if there is only one transmitter, to share it back and forth between parties. Further, fewer physical components are needed if done this way. The mirroring device is connected to the display and does not need to be removed.

A concern with this type of connection, similar to the wireless HDMI system, is that the computer or tablet the attorney is using must be compatible, or supported, by the mirroring device. Two popular types of computer operating systems are Windows and Mac (aka Apple). If the company that makes the mirroring device doesn't have software for a particular operating system, then the user is quite literally left to his or her own devices. Further, these mirroring devices require a Wi-Fi connection, unlike the wireless HDMI system.

Conclusion

Technology has the ability to allow attorneys to operate more effectively and efficiently in the courtroom. In this digital age, technology is becoming more a necessity than a novelty. The sooner it is embraced, albeit with caution and care, the sooner the legal community will reap its rewards.

Focusing on technology within the courtroom and implementing these sys-

tems allows us to better understand technology's benefits and difficulties, paving the way for greater and safer technological advances in the future. Remember, though, even with the best systems available, a good lawyer will always have a backup plan in place in case problems arise.

Do not wait until the day of trial or hearing to check the compatibility of your equipment to the Courthouse system that will be available to you during your presentation. To borrow a line from a standard Superior Court jury instruction, find out ahead of time if your equipment, the software, connections and system requirements will work together "so as to make one harmonious story of it all." Del. Super. P.J.I. Civ. §23.9 (2000).

Whenever possible, take a trip to the Courthouse and give it a trial run before the date of your presentation.⁹ This will give you the opportunity to work out any technical problems before the big day arrives. Finally, have a contingency plan in case there is a system failure and/or the trial judge decides to halt any use of technology. ♦

NOTES

1. Courts are moving forward with the use of technology in the courtroom. In some jurisdictions, for example, the U.S. District Court for the Northern District of California, the court requires the attorneys to utilize wireless servers and will not even allow connection to the network through a cable connection or tie-in.
2. Del. Lawyers' R. Prof'l Conduct 1.6 cmt. 16.
3. *Id.* at cmt. 17.
4. *Id.*
5. *Id.*
6. www.cand.uscourts.gov/wifi ("The Court makes Wi-Fi available to persons doing business with the court in all Northern District court locations. Users must have a compatible wireless-enabled device to connect to court Wi-Fi; no wired connections are allowed.")
7. Press Release, Ministry of Justice, Damian Green: 'Digital Courtrooms' to roll out nationally (June 28, 2013).
8. See Hon. Herbert B. Dixon, Jr., *The Evolution of a High-Tech Courtroom*, National Center for State Courts at page 3, 2011, <http://www.ncsc.org/sitecore/content/microsites/future-trends-2011/home/Technology/1-4-Evolution-of-high-tech-courtroom.aspx>.
9. Generally, the Court will work with the parties on access to technology. In the Superior Court of the State of Delaware, for example, the parties may contact the Bailiffs' Office to set up a time to do a trial run with technology.

Accessing Email

Busy lawyers need access to email 24/7. This means there will be multiple methods of access on multiple platforms inside and outside of the office. Each entry point has its own set of vulnerabilities. There are a number of basic steps lawyers can take to reduce the risk of breach:

In the office, keep workstations secure. Many data breaches are from threats inside the office by company employees. Keep passwords private and lock your workstation before walking away. Ensure that passwords are not kept in files on desktops named "Passwords."

iPhones and android devices are now ubiquitous in law firms. Handheld devices must be secured with passwords. If possible, the number of remote devices that can connect to the email server should be limited. Mobile Device Management (MDM) systems can track handheld devices and ensure complex passwords are enforced. An MDM can also limit applications that the firm deems inappropriate or dangerous.

**In the office, keep
workstations secure.
Many data breaches are
from inside the office
by company employees.
Keep passwords
private and lock your
workstation before
walking away.**

Healthy security behavior should be encouraged. Applications such as LastPass help to encourage password diversity and also focus employees on the importance of

protecting information.

Firms that allow web-based access to email should require dual factor authentication. Dual factor authentication requires two levels of authentication such as a password and a pin code. The pin code can be sent to a cell phone or delivered via an app on a cell phone. Web-based email can also be a concern if accessing firm email from a public computer. Web-based email may write email to temporary internet space that can remain on the hard drive after log-off.

Conclusion

Clearly, security in the use of email is the first line of defense in protecting client information. Lawyers have an obligation to remain reasonably informed on current risks associated with the use of email and the methods available in reducing the risks. ♦

NOTES

1. Ponemon Institute© Research Report 2016.
2. <http://www.nbcnews.com/politics/2016-election/email-shows-how-podesta-account-may-have-been-hacked-n674811>.

Presented by:

**Bank of America
Merrill Lynch**

KEYNOTE SPEAKER
Phil Clemens, Former CEO
Hatfield Quality Meats
Clemens Family Corporation

**DELAWARE
BUSINESS TIMES****AMERICA'S
SBDC
DELAWARE**

Family Business Growth and Stability over Multiple Generations

2017 Family Business Development Series – Part 1

Sponsored by:



Join us for the first of three events in the Delaware Business Times SBDC Family Business Development Series with special guest speaker Phil Clemens. Phil is recently retired as the CEO of all the businesses in the Clemens Family Corporation including Hatfield Quality Meats. He will share valuable information on his experience in keeping the family business together, growing and stable over multiple generations. Designed to challenge, inform and engage, this breakfast event is appropriate for family business executives of all size family businesses, attorneys, accountants and financial planners.

Visit www.delawarebusinesstimes.com/event/sbdc
to purchase tickets. For Event Sponsorships Contact:
advertising@DelawareBusinessTimes.com or call 302.504.1276

Tuesday | March 7 | 7:30am–10:00am
University and Whist Club, Wilmington, DE

OF COUNSEL: Judge Steven L. Butler

For more than a decade, Judge Steven L. Butler has been one of the most technologically savvy members of the Delaware Bar. He has been a dedicated leader in educating Delaware lawyers and judges in the use of technology and related ethical issues.

While this “Of Counsel” page of *Delaware Lawyer* is often associated with more senior members of the Delaware Bench and Bar, the editors of this issue find it most appropriate to give a “double click” to this most vocal proponent of the proper use of mobile technology in the legal profession. In 2016, Steven L. Butler accepted a life-long appointment as an Administrative Judge in the Social Security Administration.

What You Already Know

With a special interest in mobile technology, Judge Butler is best known for leading the monthly iPad Lawyers User Group (IPLUG) meetings, his proliferation of technology blogs and his well-attended and very entertaining — and at the same time somewhat scary — CLE’s for the Bench and Bar throughout the State. An advocate of both mobile platforms, Apple and Android, his goal has been inclusive rather than an effort to “turn” interested lawyers to a preferred operating system.

What You May Know

Judge Butler received his B.A. in Political Science, *magna cum laude*, from the University of Delaware in 1998, and his J.D., *magna cum laude*, from then Widener University, and now Delaware Law School, in 2003. During the hiatus between degrees, he worked in the technology field for the State of Delaware in the Judicial Information Center.

Once in private practice, Judge Butler developed a well-deserved reputation as a preeminent Social Security lawyer. For a



number of years, while with the law firm of Linarducci and Butler PA, he served his clients in the very same building in which the Social Security administrative proceedings were held. Later he broadened his practice as part of the personal injury practice group of Morris James LLP.

While providing these needed services to his clients, he developed a national reputation of managing and presenting all claims and hearings from his iPad, to the amazement of lawyers and clients alike.

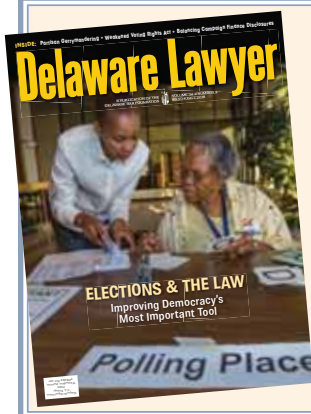
What You May Not Know

In addition to providing practical guidance and advice as a member of the Richard K. Herrmann Technology Inn of Court, Judge Butler also was selected by the Delaware

Supreme Court to be a member of the Delaware Supreme Court’s Commission on Law and Technology, where he served for three years as chair of the Mobile Technology Working Group.

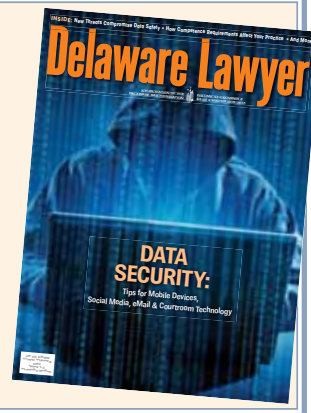
In addition to serving on the panels of dozens of Bar-related CLE’s, Judge Butler was on the adjunct faculty of the National Judicial College, leading monthly groups of judges on the use and advancements of mobile technology in the judicial field. He also contributed his time as a regular guest lecturer on mobile technology at Delaware Law School. His printed articles have been read in the Delaware Bar Association’s *The Journal* and in *Delaware Lawyer*. His digital articles have been published and republished on a number of nationally read blogs.

Judge Butler’s technology prowess within the Delaware Bar goes unchallenged. His depth and understanding of the benefits and risks of mobile technology, particularly among small law firms and solo practitioners, continues to be an incredible resource to us all. ♦

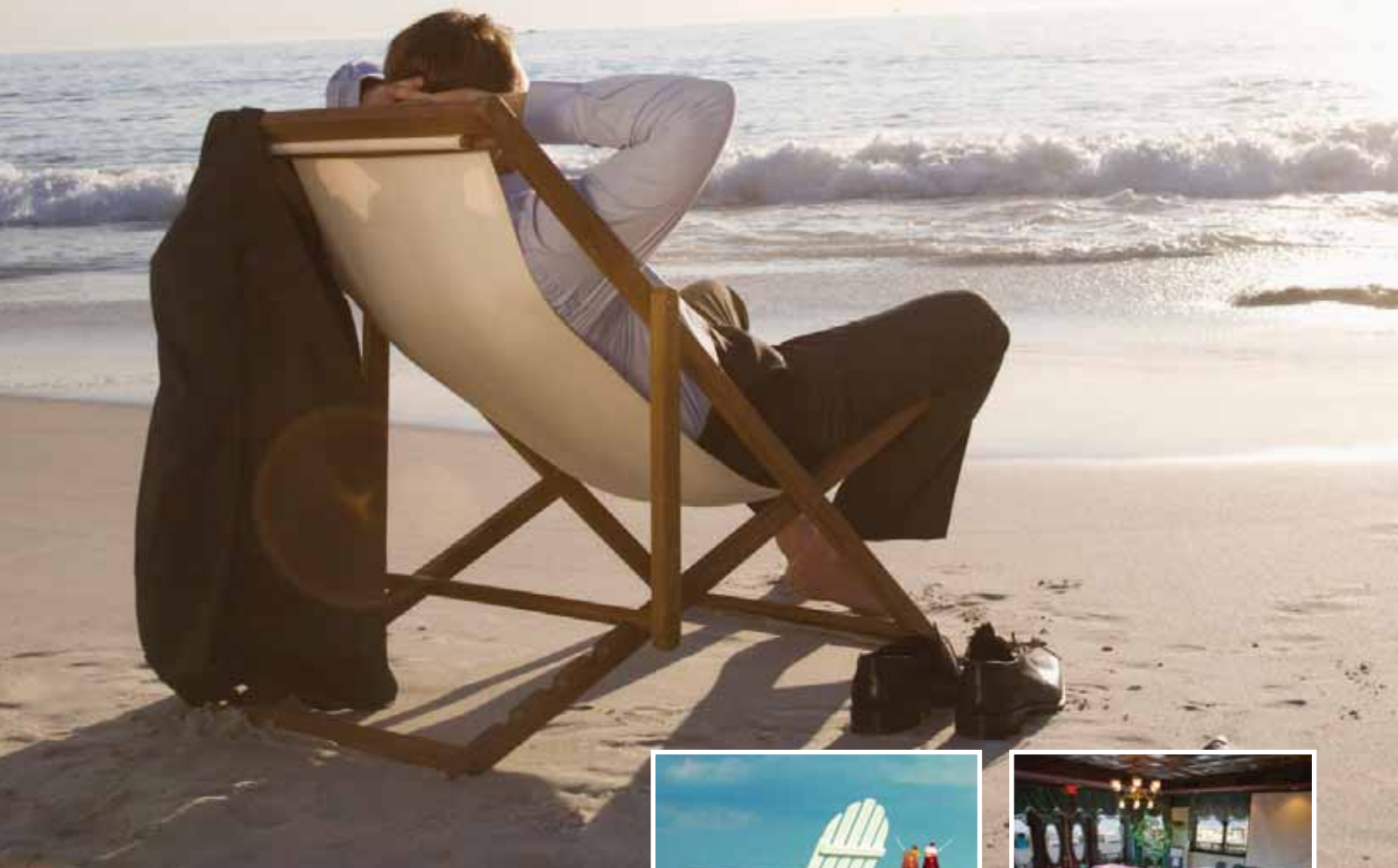


JOIN THE CONVERSATION

To learn more about *Delaware Lawyer* or the possibility of joining our volunteer Board of Editors, please contact Bar Foundation Executive Director Missy Flynn at 302-658-0773.



*It doesn't feel like work
when you're at the beach*



2 Olive Avenue & the Boardwalk
Rehoboth Beach, DE 19971
(800) 33 BEACH | (302) 227-7169
www.boardwalkplaza.com

The Boardwalk Plaza is fortunate to call the ocean's edge our home, and happy to offer you a unique and comfortable respite from the world, where you can truly get away from it all.

Both the Hotel and Victoria's are open year-round. You pick the season that suits you best, and we'll take care of the rest. Call (800) 33 BEACH.





DoubleTree by Hilton Downtown Wilmington Legal District

Now featuring 2 fully functional law centers located within one block of both the Federal and Superior Courthouses. Our 2 turnkey centers exceed 3,000 square feet in size and incorporate all of the following features:

- * 2 private lead attorney offices
- * Large War Room space with 52" HD flat screens
- * 3 large administrative workstations
- * 4 paralegal workstations accommodating up to 8 people
- * Oversized file storage rooms complete with shelving
- * Kitchen areas complete with full-size refrigerator, microwave, coffee maker and water cooler
- * Direct-dial speakerphones with voicemail at each workstation
- * Private, secured entrances with key card access
- * 100 MG dedicated Internet service in each center
- * Dedicated IT locations in each center



Second Floor
Sandra Day O'Connor Legal Suite



First Floor
Thurgood Marshall Legal Suite
Newly renovated!

For all your trial team needs contact:
Doubletree Sales Department
302.655.0400

**Call to schedule a
site tour today!**


DOUBLETREE
BY HILTON™
DOWNTOWN WILMINGTON
LEGAL DISTRICT

©2009 Hilton Hotels Corporation

700 North King Street • Wilmington, DE 19801
Reservations: 1.800.222.TREE Hotel Direct: 302.655.0400
www.WilmingtonDowntown.DoubleTree.com