Ethics and Law Firm Technology

BILL RAMSEY, NEAL & HARWELL

PHIL HAMPTON, LOGICFORCE

ABA Model Rule 1.1

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

"[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all [CLE] requirements to which the lawyer is subject.".

Technical Competence

The Washington Post

Capital Business

Lawyers, could you pass this test?

Ima ge with

By **Catherine Ho**
Reporter

Feb. 23, 2015 7:00 a.m. CST

Casey Flaherty, a law firm associate-turned-in-house lawyer-turned entrepreneur, knows firsthand how much time lawyers waste. Most bill hundreds of dollars an hour, and the longer they take to do something, the more they can charge for it.

Flaherty set out to change this. He left his job as an attorney at Kia Motors America this month to work full-time developing a test that could pressure attorneys at law firms to work more efficiently when it comes to everyday tasks like making use of Microsoft Word and Excel.

https://www.washingtonpost.com/news/capital-business/wp/2015/02/23/lawyers-could-you-pass-this-test/

What Is Technical Competence?

- Casey Flaherty, Procertas
- Legal Technology Assessment (LTA)
- Used by corporate legal departments to assess outside counsel
- Measures proficiency in Word, Excel, PDF
- www.procertas.com

Know "Benefits and Risks" of Technology

Benefits

- Productivity Software
- Organization and Collaboration Systems
- Case/Client Management
- Cloud Technology

Attorneys Ethical Duty To Exercise Good Time Management

ABA Model Rule 1.3

"A lawyer shall act with reasonable diligence and promptness in representing a client"

ABA Rule 1.3

Comment[2]:

"A lawyer's workload must be controlled so that each matter can be handled competently"

Comment[3]: Warns against procrastination

"A client's interest often can be adversely affected by the passage of time…"

Malpractice Warning Signals*

Failure to make and follow a priority task list

Disorganized office

Disorganized files

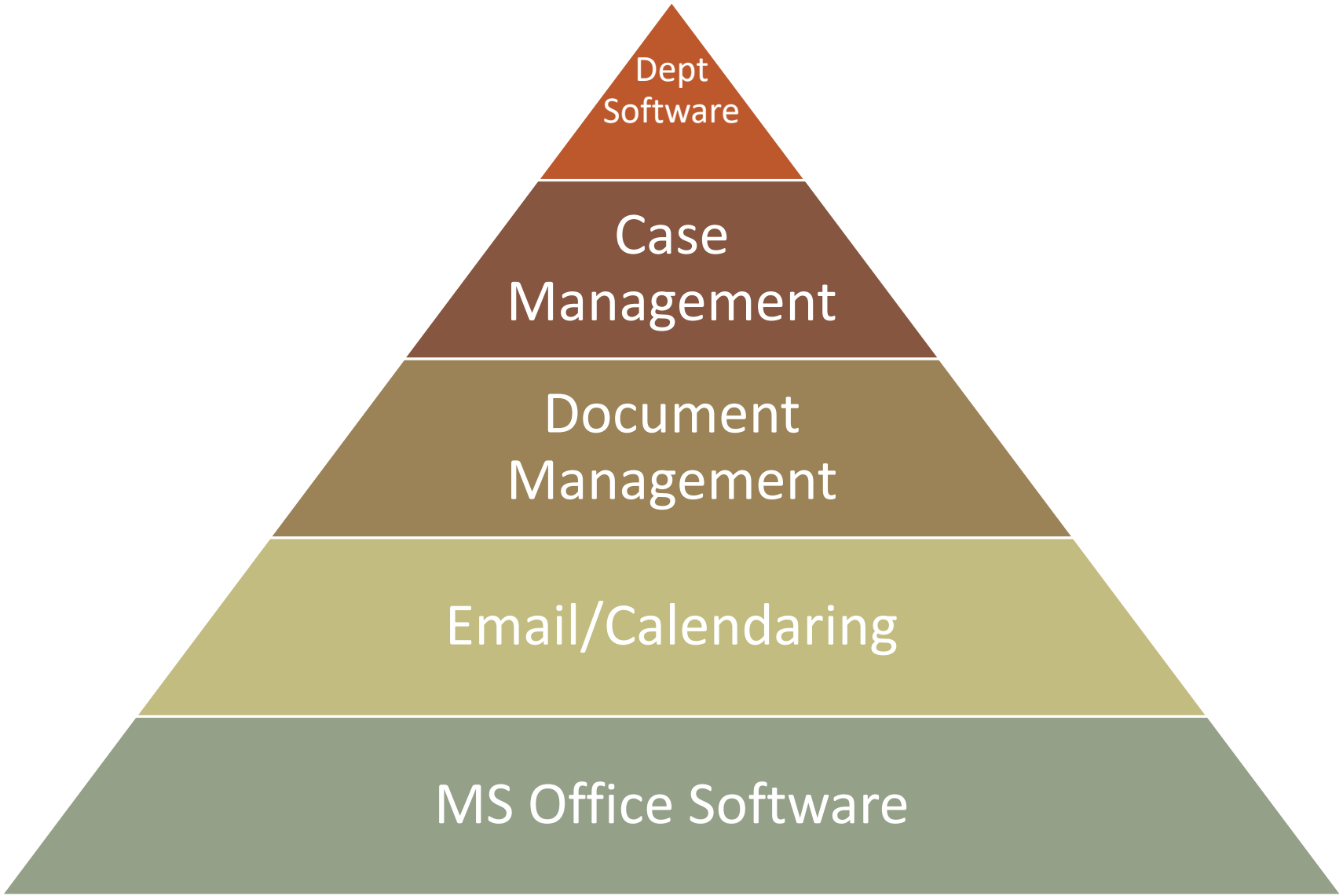
Failure to keep personal calendar

Sloppy timekeeping

* "Malpractice Warning Signals," Bar Association of the District of Columbia Monthly Newsletter (Vol. 1, Issue 4, April 1996), citing Nancy Byerly Jones, Director and Practice Management Counsel for the North Carolina State Bar

Microsoft Office 365 Business

- Full desktop software applications
- $99/user/year (install on up to 5 PCs/laptops)
- 1TB OneDrive storage/user
- Full mobile app access on up to 5 mobile devices
- 300 user maximum
- vs MS Office 2019


Dept Software
Case Management
Document Management
Email/Calendaring
MS Office Software

What About The Cloud?

Modern day "cloud computing" concept introduced by Google CEO Eric Schmidt in 2006

Law firms slow to adopt

Ethical considerations

- Security/privacy of client data
- Ownership of data
- Reliability of cloud vendor

Model Rule 1.6(a): Confidentiality of Information

A lawyer shall 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 by paragraph (b).

Model Rule 1.6(c): Confidentiality of Information

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

ABA Formal Opinion 477

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. … The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure

Comment [18] to Model Rule 1.6(c)

- "Process" to assess risks
- Identify and implement appropriate security measures responsive to risks
- Verify they are effectively implemented
- Ensure they are continually updated in response to new developments

--ABA Cybersecurity Handbook

Factors in Determining Reasonableness of Efforts

- Sensitivity of information
- Likelihood of disclosure if additional safeguards not employed
- Cost of employing additional safeguards
- Difficulty of implementing safeguards
- Extent to which safeguards adversely affect lawyer's ability to represent clients

E-mail Communications

Opinion 99-413 (1999):

- "Lawyers have reasonable expectation of privacy in communications made by all forms of e-mail…despite some risk of interception and disclosure"
- Consistent with "reasonable means" in Rule 1.6

Unencrypted e-mail still acceptable for routine communication with clients

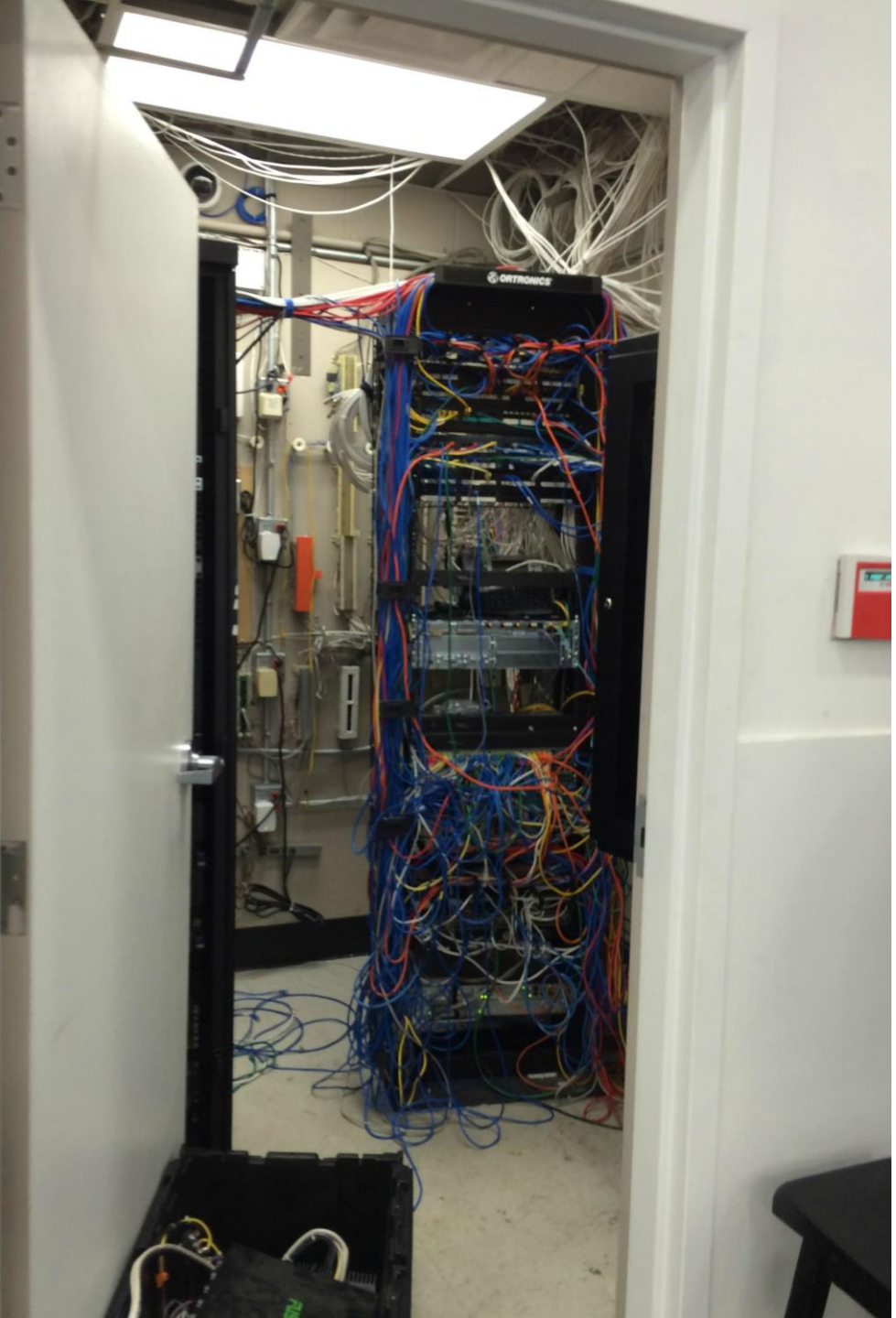
Exceptions possible on case-by-case basis

- Examples: Medical, banking, etc.

Cloud Technology

TN Ethics Opinion 2015-F-159:

- *"A lawyer may ethically allow confidential client information to be stored in "the cloud" if the lawyer takes reasonable care to assure that: (1) all such information or materials remain confidential; and (2) reasonable safeguards are employed to ensure that the information is protected from breaches, loss, and other risks. Due to rapidly changing technology, the Board doesn't attempt to establish a standard of care, but instead offers guidance from other jurisdictions."*



Evolution to the Cloud

Evolution to the Cloud

The Serverless Law Firm

Know "Benefits and Risks" of Technology

Risks

- Cybersecurity/Privacy
- Social Media
- Texting
- Mobility

2019 Verizon DBIR Report Summary

- As business migrates to the cloud, phishing and credential theft have risen as attack mode
- 94% of malware infections delivered via e-mail
- Users are much more susceptible to social attacks when using mobile devices

2019 Verizon DBIR Report Summary

43%

of victims are small business

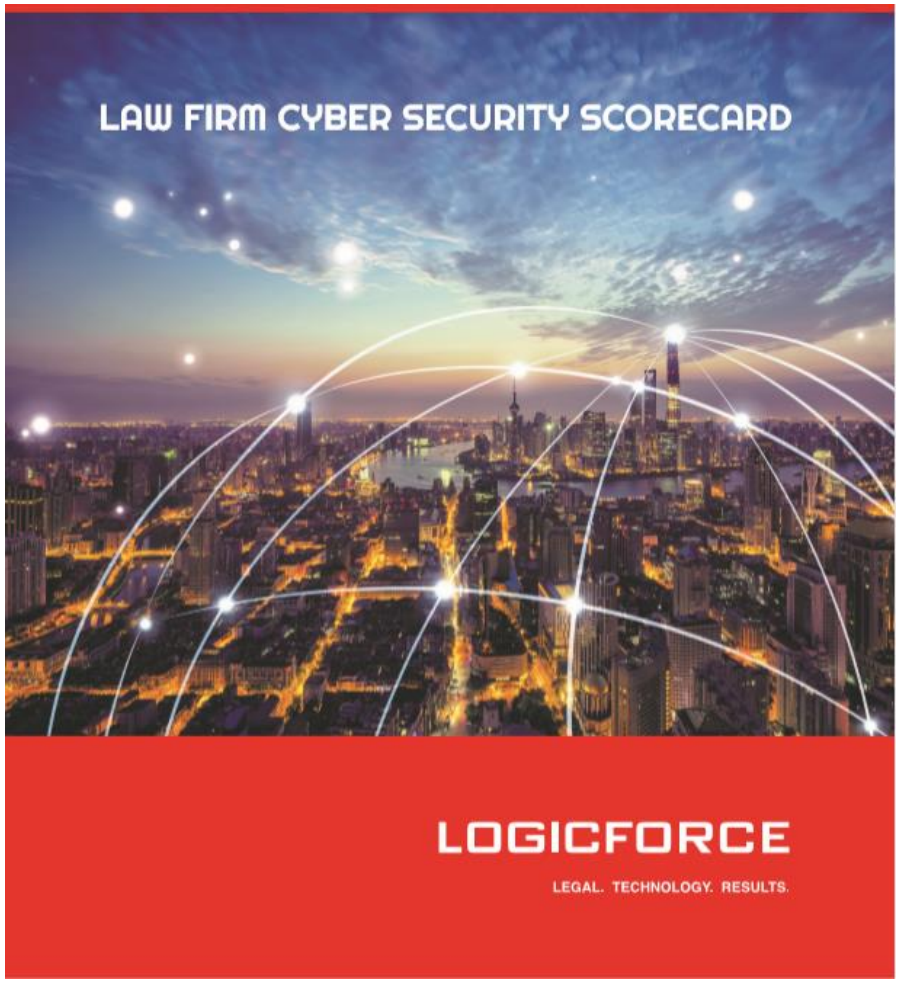
$25,000

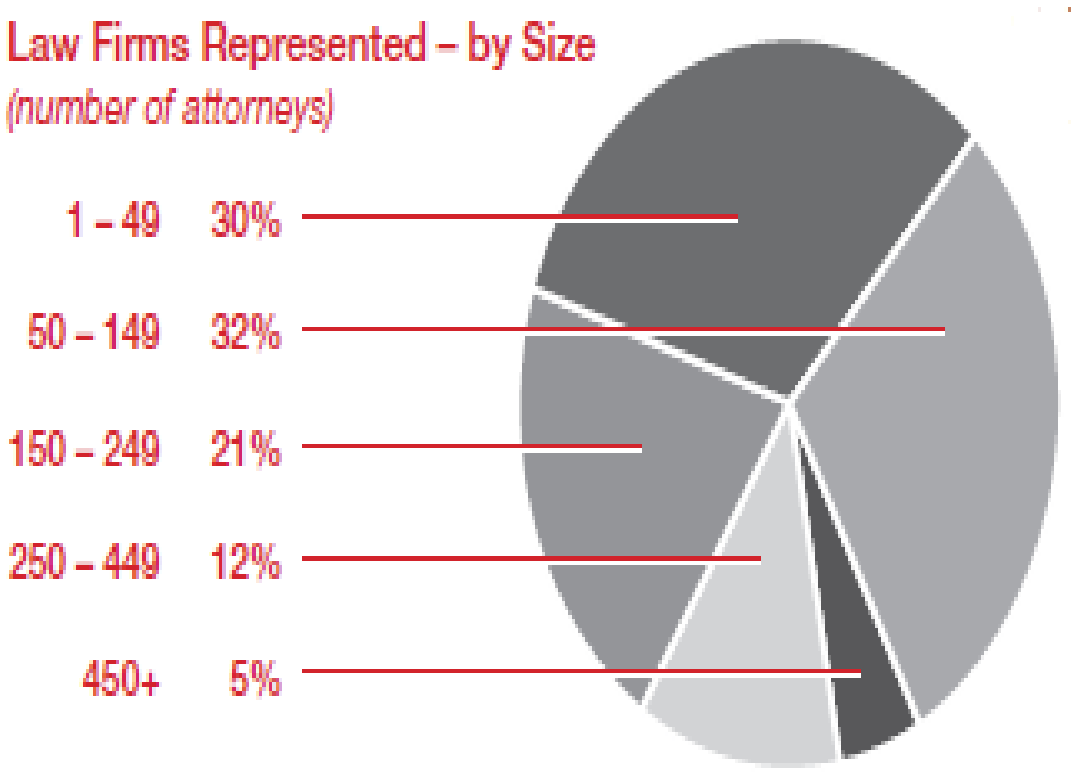
Median direct impact for business email compromise

~80%

Fraudulent transactions in professional service firms involved pretexting

LOGICFORCE 2019 CyberSecurity Scorecard





LOGICFORCE CyberSecurity Report Card

200

U.S. law firms surveyed

51%

Had data security practices audited in past year

2%

of firm revenue: minimum recommended spend on cybersecurity

2019 CyberSecurity Scorecard

THE LEGAL INDUSTRY SCORE INCREASED SLIGHTLY IN 2019

The 2019 legal industry score for cybersecurity health is 60.1%. While we see some improvement in cybersecurity leadership and governance, law firms are behind on more advanced measures such as DLP, multi-factor authentication, and records management.

CATEGORIES	WEIGHTED VALUE	2019 WEIGHTED AVERAGE	2019 IMPLEMENTATION SCORE	2018 IMPLEMENTATION SCORE
Cybersecurity investment	5%	5	100%	99%
Password management security	5%	4.9	98%	99%
3rd party risk assessment	10%	9	90%	-
Penetration testing	5%	4.3	86%	-
Vulnerability testing	5%	4.15	83%	-
Cybersecurity policies	5%	3.5	70%	55%
Formal training	10%	6.8	68%	54%
Cybersecurity insurance	5%	3.05	61%	65%
Records management policy	5%	2.7	54%	65%
Proper security executive	10%	4.9	49%	34%
Full disk encryption	5%	1.95	39%	40%
Multi-factor authentication	15%	5.4	36%	47%
Monitoring (SOC)	10%	3.4	34%	24%
DLP technology	5%	1.05	21%	47%

2019 INDUSTRY SCORE 60.10%

2018 INDUSTRY SCORE 54.25%

12 Cybersecurity Standards

1. Information security executive
2. Cybersecurity policies and backup procedure
3. Multi-factor authentication
4. Cyber training
5. Cyber insurance
6. Penetration and vulnerability testing

-2019 LOGICFORCE Cybersecurity Scorecard

12 Cybersecurity Standards

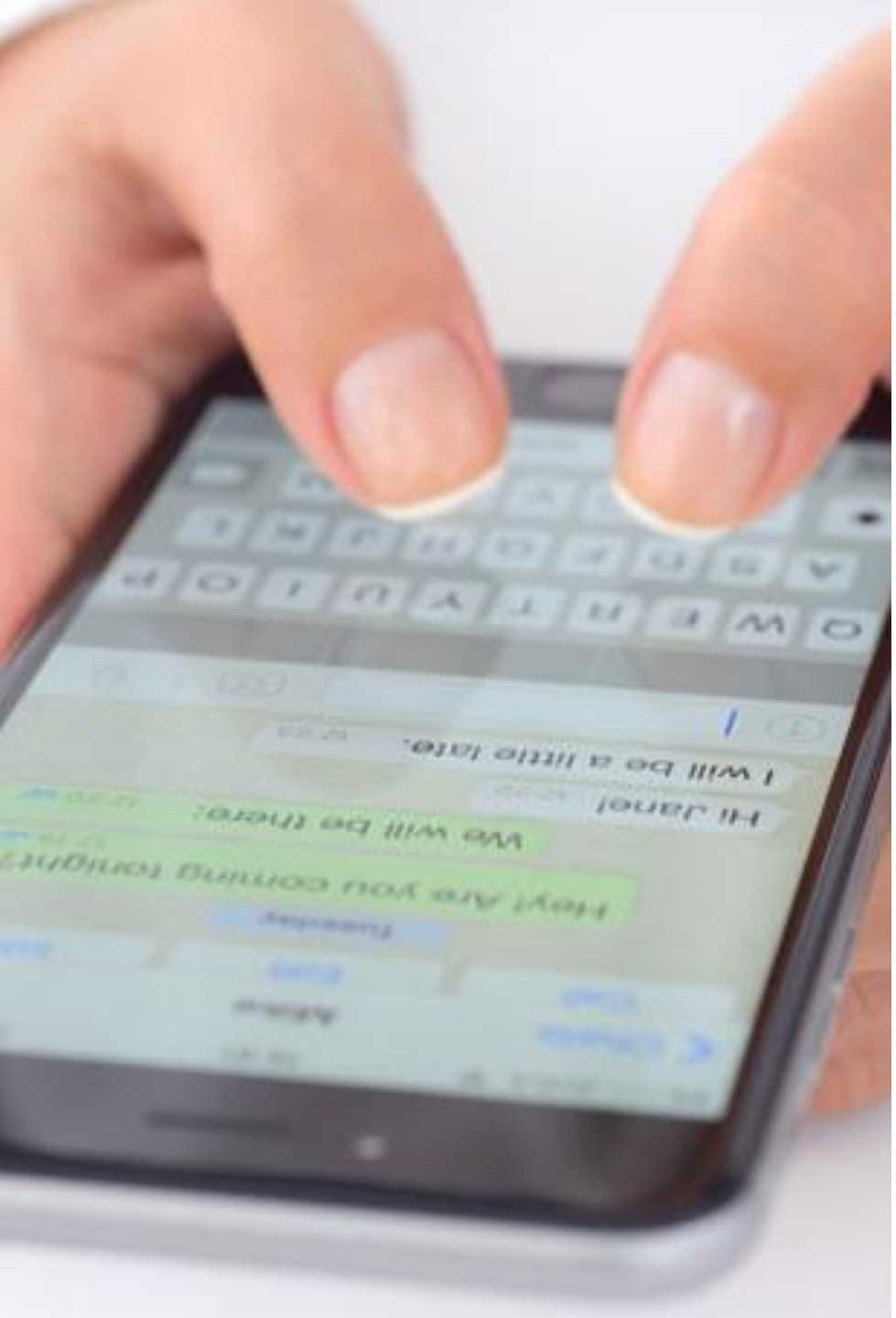
7. Password management tool
8. Records management policy
9. Security Operations Center (SOC) monitoring
10. Full Disk Encryption (FDE)
11. Data Loss Prevention (DLP) services
12. Third-party risk assessments

-2019 LOGICFORCE Cybersecurity Scorecard

Risks: Social Media Use

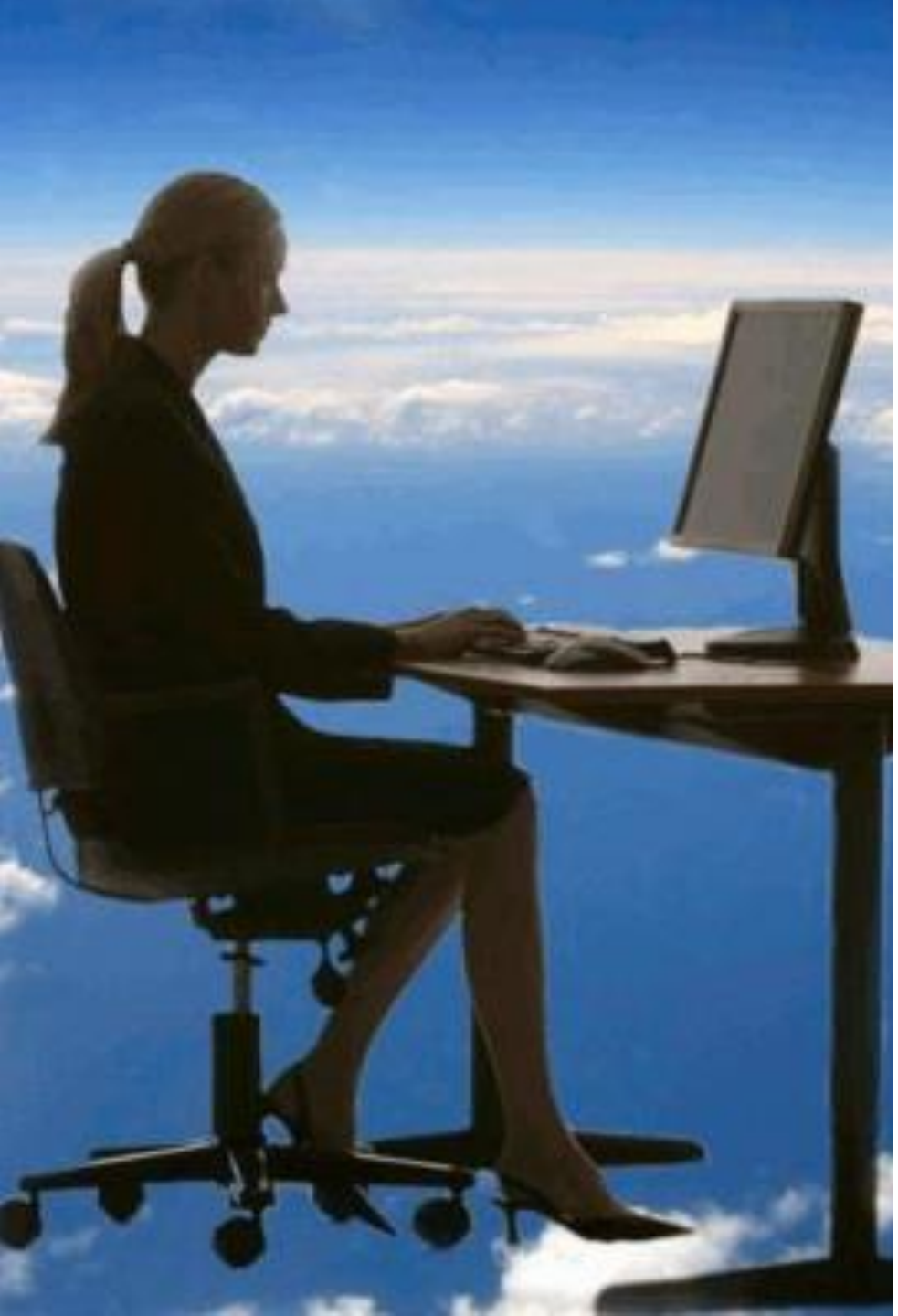
- Social media policy training
- Bad idea to use social media platforms for confidential communications
- Twitter posts can be a headache as they might reveal strategy or biases of the attorney
- Friending represented parties to gain information has been found to be unethical
- Friending under false pretenses has been found to be unethical
- Don't neglect social media in electronic discovery
- Monitoring jurors' social media use

John G. Browning, *Keep Your "Friends" Close and Your Enemies Closer: Walking the Ethical Tightrope in the Use of Social Media*, 3 ST. MARY'S J. LEGAL MAL. & ETHICS 204(2013) (http://lawspace.stmarytx.edu/item/Browning_final.pdf)



Risks: Texting

- Accepted form of business communications today
- Ignoring client texts can be violation of ethics rules
- Texting as a form of advertising



Risks: Mobility

- Cloud technologies allows for virtual law office
- Not every "virtual office" is safe
  - Dangers of open Wi-Fi
  - VPN
- Safeguards
  - Multi-factor authentication
  - Strong password management
  - Remote wipe capability
  - Encryption

THANK YOU!

Any questions?

E-mail us at
ramseywt@nealharwell
phampton@logicforce.com