Cyber Due Diligence in Mergers and Acquisitions: Finding Risks

Shawn E. Tuma
Co-Chair, Data Privacy & Cybersecurity Practice
Spencer Fane LLP
www.spencerfane.com
stuma@spencerfane.com
o: 972.324.0317
m: 214.726.2808

SpencerFane

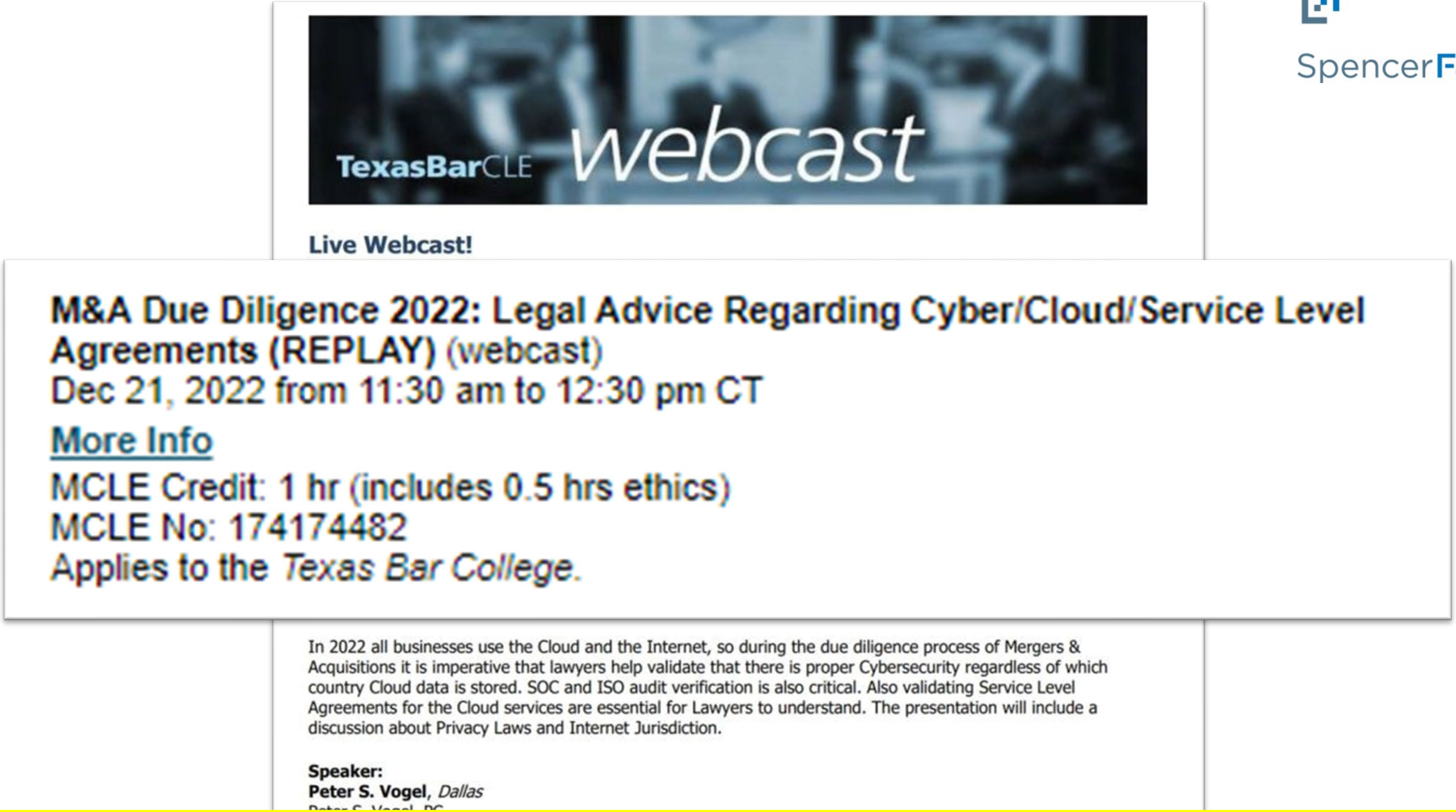
Cyber risk is not just technical “IT risk”
Cyber is an overall business risk

SpencerFane®

The Objectives

Two main components for addressing cyber risk in M&A transactions:

1. The documents – the agreements, obligations, representations, warranties, disclosures, reps/warranties insurance, etc.
2. The actual cyber risk of the company – its real-world cyber risk posture – *i.e.*, how likely is it going to have an incident, how will it impact the company, and how much will it cost?



Live Webcast!

M&A Due Diligence 2022: Legal Advice Regarding Cyber/Cloud/Service Level Agreements (REPLAY) (webcast)
Dec 21, 2022 from 11:30 am to 12:30 pm CT

More Info

MCLE Credit: 1 hr (includes 0.5 hrs ethics)
MCLE No: 174174482
Applies to the *Texas Bar College*.

In 2022 all businesses use the Cloud and the Internet, so during the due diligence process of Mergers & Acquisitions it is imperative that lawyers help validate that there is proper Cybersecurity regardless of which country Cloud data is stored. SOC and ISO audit verification is also critical. Also validating Service Level Agreements for the Cloud services are essential for Lawyers to understand. The presentation will include a discussion about Privacy Laws and Internet Jurisdiction.

Speaker:
Peter S. Vogel, *Dallas*
Peter S. Vogel, PC

http://www.texasbarcle.com/CLE/AABuy1.asp?bOverride=&sProductType=EV&lID=21201&Code=&O=&bHitCounted=0

The Objectives

Better understand the actual cyber risk of the company – its real-world cyber risk posture – i.e., how likely is it going to have an incident, how will it impact the company, and how much will it cost?

In a nutshell, what are we trying to figure out?

SpencerFane®

Does the company have an adequate understanding of its own cyber risk posture?

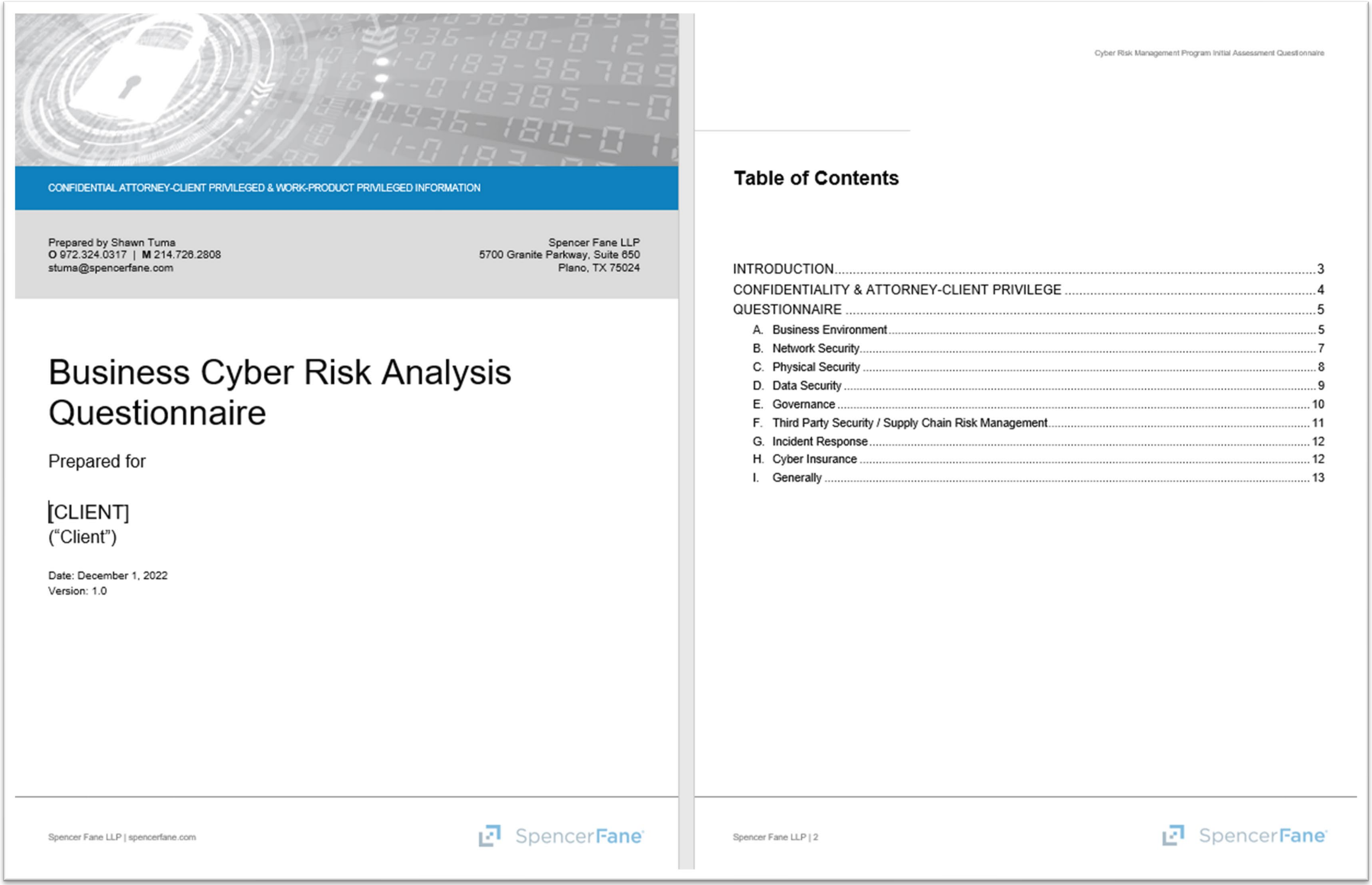
Does the company have a plan for mitigating its risks in a prioritized and systematic manner?

Is the company effectively executing that plan and continuing to mature this process?

Most do not.

The Process

1. In an ideal world, we will have plenty of time and resources and could treat this like a proactive cyber risk management engagement. The better we understand the company, the better we can understand its risks.



CONFIDENTIAL ATTORNEY-CLIENT PRIVILEGED & WORK-PRODUCT PRIVILEGED INFORMATION

Prepared by Shawn Tuma
O 972.324.0317 | **M** 214.726.2808
stuma@spencerfane.com

Spencer Fane LLP
5700 Granite Parkway, Suite 650
Plano, TX 75024

Business Cyber Risk Analysis Questionnaire

Prepared for

[CLIENT]
(“Client”)

Date: December 1, 2022
Version: 1.0

Spencer Fane LLP | spencerfane.com

SpencerFane

Cyber Risk Management Program Initial Assessment Questionnaire

Table of Contents

Spencer Fane LLP | 2

SpencerFane

The Process

1. In an ideal world, we will have plenty of time and resources and could treat this like a proactive cyber risk management engagement. The better we understand the company, the better we can understand its risks.
2. In the real world, that’s usually not going to be the case. We will likely have a short timeframe, limited appetite for questions and analysis, and a limited budget.
3. The size of the deal, nature of the parties, and timing considerations will all impact the extent of your analysis.
4. It may come down to just a couple of questions on a half hour call, if that.
5. In the end, hopefully, it will result in a conversation.

Overview – where are we looking?

- Business Environment
- Network Security
- Physical Security
- Data Security
- Governance
- Third Party Security / Supply Chain Risk Management
- Incident Response
- Cyber Insurance

Risk Assessment

The most essential step?

- How do you protect against what you don't know?
- How do you protect what you don't know you have?
- How do you comply with rules you don't know exist?
- Demonstrates real commitment to protect, not just "check the box compliance."
- No two companies are alike, neither are their risks, neither are their risk tolerances.

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." –*Sun Tzu*

Data Map

The most essential question?

Do you have a Data Map that includes both sensitive personal information and sensitive business information?

Top 10 Magic Questions

What are the Top 10 "Magic" Questions you can ask?

i.e., where is the Easy Button?

THERE ARE NO MAGIC QUESTIONS!

YOU ARE TRYING TO UNDERSTAND RISK!!!

YOU MUST HAVE SOME UNDERSTANDING OF THE COMPANY TO KNOW WHAT QUESTIONS APPLY!!!

16 Pretty Good Questions

1. Does the company perform a risk analysis, risk assessment, or some other process to better understand its greatest risks?
2. Does the company have a Data Map?
3. Does the company have policy requiring unique passwords for all members of the workforce to access the network?
4. Does the company require Multi-Factor Authentication (MFA) for all remote access and administrative or privileged accounts – especially MS O365?
5. Does the company require cybersecurity awareness and phishing training and exercises for all members of the organization, especially senior leadership?
6. Does the company use Remote Desktop Protocol (RDP) or have public facing RDP blocked in the environment?
7. Does the company backup its data and configurations, regularly test them, and keep at least one copy of the backups offline, such as with the “3-2-1 backup” process?
8. Does the company use email filtering technology?
9. Does the company use device encryption for all portable devices to ensure that if it is lost or stolen, its confidentiality is not compromised?
10. Does the company update and patch its systems promptly, especially external-facing systems, and configure automatic updates on workstations and laptops where feasible?
11. Does the company de-escalate privilege to the minimum necessary on user accounts, especially for high value target users such as executives, IT administrators, accounting, human resources, and for vendor access?
12. Does the company use a reputable firewall?
13. What endpoint detection solution does the company use?
14. What network monitoring solution does the company use?
15. Does the company have an incident response plan or what other incident response preparation has the company engaged in?
16. Does the company have cyber insurance?

Information to Request

1. Data Map (including both sensitive personal information and sensitive business data)
2. Asset Inventory & BYOD Policy
3. Internal and external facing Privacy Policies and/or Privacy Notices
4. Terms of Use for website
5. Data Retention / Destruction Policy
6. Backup Policy
7. Password Policy
8. Access Control Policy
9. Acceptable Use Policy
10. Employee Handbook provisions relating to data / cyber / privacy types of issues
11. Data Classification Policy

11. Data Loss Prevention Policy
12. Policy and Materials for Workforce Training
13. Written Information Security Program / Cybersecurity Risk Management Program
14. Incident Response Plan
15. Third-Party Service Provider Policy / Assessments
16. Risk Assessments
17. SOC reports
18. Cyber / Privacy Risk Insurance policy
19. Master Services Agreement sample language (or other agreements with customers affecting data responsibilities and obligations)
20. Any other similar information that may not have been listed but may be relevant to this analysis

Only 1 Question

Source: Derek Keats https://flickr.com/photos/93242958@N00/34631274655

Does the company have cyber insurance?

Thank you!

SpencerFane

Shawn Tuma

Co-Chair, Cybersecurity & Data Privacy

Spencer Fane LLP

972.324.0317

stuma@spencerfane.com

SpencerFane®

- 20+ Years of Cyber Law Experience
- Practitioner Editor, Bloomberg BNA – Texas Cybersecurity & Data Privacy Law
- Council Member, Southern Methodist University Cybersecurity Advisory
- Board of Advisors, North Texas Cyber Forensics Lab
- Policy Council, National Technology Security Coalition
- Board of Advisors, Cyber Future Foundation
- Cybersecurity & Data Privacy Law Trailblazers, National Law Journal (2016)
- SuperLawyers Top 100 Lawyers in Dallas (2016)
- SuperLawyers 2015-21
- Best Lawyers in Dallas 2014-21, D Magazine

- Past Chair, Computer & Technology Section, State Bar of Texas
- Privacy and Data Security Committee of the State Bar of Texas
- College of the State Bar of Texas
- Fmr Board of Directors, Collin County Bench Bar Conference
- Past Chair, Civil Litigation & Appellate Section, Collin County Bar Association
- Information Security Committee of the Section on Science & Technology Committee of the American Bar Association
- North Texas Crime Commission, Cybercrime Committee & Infragard (FBI)
- International Association of Privacy Professionals (IAPP)