



# COMPUTER AND TECHNOLOGY SECTION



## SECTION LEADERSHIP

### CHAIR

Joseph Jacobson

### CHAIR-ELECT

Eric Griffin

### SECRETARY

Michael Curran

### TREASURER

Shannon Warren

### NEWSLETTER EDITOR

Michael Curran

### ASST. NEWSLETTER EDITORS

Craig Ball & Antony P. Ng

### IMM. PAST CHAIR

Antony Ng

### COUNCIL MEMBERS

Craig Ball

John G. Browning

Sammy Ford IV

Reginald A. Hirsch

Laura Candice Leonetti

Daniel Lim

Elizabeth Rogers

Shawn Tuma

Bert Jennings

### BOARD ADVISOR

Grant Scheiner

### ALT. BOARD ADVISOR

Robert Guest

# Circuits

Newsletter of the Computer & Technology Section  
of the State Bar of Texas

Volume 3: Winter 2015

## TABLE OF CONTENTS

<b>Letter from the Chair – ILTA Announcement</b>	2
By Joseph Jacobson	
<b>Letter from the Editor</b>	5
By Michael Curran	
<b>Practical Cyber Law: Yes, Even Your Clients May Face Cyber Risk Issues</b>	6
By Shawn Tuma	
<b>The Corner Privacy Counselor: How to Prepare for Breach Readiness and Breach Response</b>	9
By Elizabeth Rogers	
<b>Why Law Firms Should Accept Bitcoin</b>	13
By Jason Rodriguez and Thomas Allen	
<b>How to Join the State Bar of Texas Computer &amp; Technology Section</b>	17
<b>State Bar of Texas Computer &amp; Technology Council</b>	19

## Practical Cyber Law: Yes, Even Your Clients May Face Cyber Risk Issues

By Shawn Tuma

Lawyers in different practice areas, especially those that involve business, can expect to start seeing cyber risk issues arising with their clients more frequently. While that statement may come as quite a shock to many, before going further, I recognize what you may be thinking: “but my clients are just general businesses, they are not in the high-tech business, so how does this apply to me?”

Because of the prevalence of cyber risk in today’s business environment, cybersecurity and data privacy issues arise in a wide variety of business relationships. Unless your clients do not (1) use a computer, (2) receive, store, or transmit electronic data, or (3) connect to the Internet — and do not do business with any company that does — your client’s business could be impacted by cybersecurity and data privacy issues.

If any of your clients found themselves in such a situation, oftentimes you will be their first line of defense. By having a basic understanding of these issues, you will be able to give them much better guidance, even if that guidance is simply referring them to someone who has expertise in handling the relevant issues.

### Two Real-Life Examples of How Lawyers Who Represent Business Clients Can Face Cyber Issues

The recent Target data breach provides an excellent illustration of this point. Did you know that the hackers that compromised Target’s point of sale system and stole its payment card data did not “hack” into Target’s system directly? Instead of attacking Target head-on where Target’s defenses were strongest, they followed the ancient lessons of warfare and used an indirect method of attack to strike Target where its defenses were weaker.

The hackers did this by using a common email “click here” scheme, that when opened by an unsuspecting employee of Fazio Mechanical Services, deposited malware on Fazio’s network. Fazio was one of many third-party vendors that provided HVAC services to Target. Once the hackers’ malware was on Fazio’s network, they used it to “sniff” the network and find the login credentials Fazio used to access Target’s portal that vendors used for submitting electronic billing, contracts, and project management data. This provided the hackers with their entry

point into Target's network. Once they were inside the perimeter of Target's network, they were in a much better position to unleash their attack on Target.<sup>1</sup>

Cyber risk knows no boundaries and can impact every kind of business. Target is not a technology company. Target is not involved in a particularly technology-heavy industry. Target is a retailer that was attacked because it has data that is valuable. Target uses technology in its business operations and, while that technology is a valuable asset, it also proved to be a vulnerability. Fazio is an HVAC company that is likewise not in a particularly technology-heavy industry. Fazio used technology in its business operations and, because its (likely largest) customer required it to integrate its technology, Fazio was attacked because it provided an entry point into its customer's computer network.

While your clients may not be an industry giant like Target, they could easily be an entry point to one such as a Fazio. As of the time of this writing, there is no report of Target having taken formal legal action against Fazio because of this breach but that does not mean that Target cannot or will not. Indeed, for a smaller company like Fazio, simply losing the business of a customer like Target could be enough to put the company out of business. These are serious matters. The Target case, however, is not the only example of how third parties can be used to execute such attacks and the risks that come with them.

Last year, a group of hackers were trying to hack into the network of a large oil company but were unable to breach its network with head-on attacks. Considering the indirect method of attack, after learning that a Chinese restaurant located near the company's office was popular with the company's employees, they infected the restaurant's online menu with malware. When the employees using the company's computers visited the menu, they inadvertently downloaded the malware which gave the attackers the entry point they needed into the company's computer network.<sup>2</sup>

Neither the oil company nor the restaurant was a technology company. But, one had valuable data and one was a vehicle that provided a means for gaining access to the other's computer

---

<sup>1</sup> 11 Steps Attackers Took to Crack Target, CIO Online, <http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html> (last visited Jan. 25, 2015).

<sup>2</sup> Hackers Lurking in Vents and Soda Machines, The New York Times, [http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?\\_r=0](http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?_r=0) (Apr. 7, 2014).

network. Do you have clients that have valuable data? Do you have clients that have websites or other forms of digital connections to companies that may have valuable data?

Hackers are very creative. As more companies work to strengthen their own defenses, this kind of indirect method for attacking their primary targets is becoming more common. Not only do businesses now face cyber-attacks directed at them, but now they may also face cyber-attacks because of their relationships with other businesses. The pool of potential cyber-attack victims is expanding exponentially.

### **Practical Lawyers Should Be Able to Recognize the Cyber Issues as Their Clients' First Line of Defense**

As the variety of businesses involved in cyber-attacks increases, the lawyers who represent them will start seeing more of these issues arise. As their clients' first line of defense in many cases, lawyers who have enough familiarity with cybersecurity and data privacy issues to alert their clients from the beginning will be doing them a great service. The rules and regulations of various industry groups and governmental authorities are evolving rapidly and their time for compliance can be very short. Businesses that find themselves in these situations must respond quickly. If they do not, then the consequences can be much worse.

While you may not wish to become an expert on cybersecurity and data privacy issues, it is helpful for you to be able to identify the issues well enough to recognize that someone needs to address them. In the right situation, that advice can be invaluable to your clients. That is practical lawyering in the 21st Century.

#### **About the Author**

Shawn Tuma (@shawnetuma) is a cybersecurity lawyer business leaders trust to help solve problems with cutting-edge issues involving cyber risk and compliance, computer fraud, data breach and privacy, and intellectual property law. He is a partner at Scheef & Stone, LLP, a full service commercial law firm in Texas that represents businesses of all sizes across the United States.