**ESQ RECRUITING LLC**

**Wanted: Cybercrime Fighters**

*By: Dawn Lowe*

It started out as a peaceful Saturday. Let's just say it involved a steaming cup of coffee, a roaring fire in the fireplace, and me on my laptop clicking around. I read the news, read some movie reviews, and then checked my bank account. Stop the presses… Who ordered $314 worth of software? Immediately I raced upstairs to confront the teenagers. After feuding, fussing, and a lecture about the value of money, they still denied making the purchase. My mind stopped spinning and settled on an article I read an hour earlier about the customer data breach of a certain big-box retailer. "Wait," I said to myself, "I shopped there!"

Back downstairs I raced to my laptop, confirmed that I, indeed, had shopped at said retailer during the time of the data breach. Like a film in slow motion, I read the details of the scandalous purchase and realized that someone had stolen my credit card information to purchase a $314 software download. I know the purchase occurred somewhere in the cold recesses of Russia because I was immediately billed for an exchange of currency from Rubles to US dollars. "What the heck!"

What happened next, you ask? After the fury of having my hard earned dollars stolen had subsided, I called my bank. God bless my bank. They handled the reversal of the charges and the changing of my debit cards with quickness and ease. Then came the shock that some random person in Russia got my private information and used it against me. Feeling violated doesn't quite cover the emotion that I experienced. I began to rethink how I paid for things, to whom I gave personal information, and whether or not I was better off paying for everything the good old-fashioned way…cold, hard cash.

Cybercrimes are real. Cybercriminals are real. As a matter of fact, the 2013 Cost of Cybercrime Study: United States revealed that cybercrime is up a whopping 18% over 2012. Probably adding to the 18% increase is the explosion of data storage on the cloud. Meaning that there is a whole lot more data to steal floating around on that cloud, wherever it is. With all this data storage and processing, a whole new field of law has emerged. We need attorneys involved in the protection and risk management of the massive amounts of data floating over the United States. There are also legal issues surrounding data ownership and venuing.

With such a high increase in data breaches in 2013, attorneys also play a role advising the legally appropriate way to handle the breach. In most cases, attorneys will need to collaborate with IT to come up with a data breach response plan. I predict that how a corporation communicates a data breach to it's customers or employees will become a legal matter as well.

Just fighting cybercrime is big business. The 2013 Cost of Cybercrime Study: United States also revealed that 60 larger US companies each spent up to $58 million protecting their data. Not included in the previous dollar amounts is the value of what may have been stolen; like property, customer loyalty, and income. Once these cybercriminals are caught, we need in-house attorneys and law firm attorneys to collaborate together to put away these cyber bad guys.

Are you seeing the wave of the future? You should. Technology is advancing at amazing rates and data processing and storage is THE key component. Now get in your cars and race to your local attorney placement firm, headhunter, or recruiter and get busy finding those in-house jobs fighting cybercrime. For my sake, PROTECT MY DATA!