Volume 6 - Issue 12 **December 2014**

The Franchise Valuations Reporter

Special Report on Cyber-Security

This issue of *The Franchise Valuations Reporter* is devoted to a single topic: **Cybercrime against law firms** and what is being done to counter this looming threat.

Whether you are on the legal, the supplier or the operational side of franchising, we hope this discussion enlightens and - even more important - prompts you to take action.

Bruce S. Schaeffer, Editor
Bruce@FranchiseValuations.com
212.689.0400

Our Expertise

Within the franchise, distribution and dealership context, we are experts in:

- Damages, Valuations & Expert Testimony
- Finance, Accounting and Tax
- Cyber Security and E-discovery of Electronically Stored Information

We offer a free initial consultation. If any readers have questions, you are welcome to email or phone us and we will provide our best answer as quickly as possible.

Bruce S. Schaeffer, Editor
Bruce@FranchiseValuations.com

Cyberattacks on Law Firms: A Nightmare Scenario

Why Hackers See Law Firms As Rich Targets

The following is a Q and A session between The Franchise Valuations Reporter and an independent information security professional whose practice focuses on law firms, financial services and franchising. I agreed not to identify him by name in order to protect the confidentiality of his high-profile clients.

FVR: Over a year ago, Mary Galligan, FBI special agent in charge of cyber and special operations, warned attendees at LegalTech "[w]e have hundreds of law firms that we see increasingly being targeted by hackers." Law firms have been called the soft underbelly route to stealing confidential information. **Is this just hype or is the threat real?**

InfoSec: This is absolutely a real threat. Criminals are on the lookout for low-hanging fruit and law firms are a rich source of confidential personal and business information. They see outside counsel as the way in because (1) they can gain access to files on hundreds or thousands of companies from a single point of contact and (2) security protocols at law firms tend to be weaker than their clients'. Law firms give hackers a high return on their investment.

The unfortunate truth is that many law firms are just waking up while others will continue to slumber until the fit hits the shan. Most law firm ESI (Electronically Stored Information) is minimally protected if at all. Most small- to-medium-sized law firms and franchise companies do not vigilantly secure their highly sensitive, confidential documents - either because of the expense or ignorance of the risk or both.

***FVR:* But as a lawyer myself, I crave the immediacy and convenience of instant access. I hate having to jump through hoops to get online.**

InfoSec: I see that a lot in my practice and criminals love you for it. Everyone wants instant access, 24/7, on everything including BYO mobile devices. Often the whole office uses an unsecured and unencrypted wireless network or WiFi hotspots at airports, coffee shops and hotels. Whether they use thumb drives plugged into a laptop or a smartphone connected to the Cloud, users demand unrestricted mobility whether they work from home or on the train. But that is super dangerous and just having antivirus software and a firewall is not enough.

Accidental data spills do happen. For example, a few years back there was an incident where an employee of a Maryland law firm left an unencrypted portable hard drive containing medical data and case information on a train and it was never recovered.

***FVR:* Other than a few high-profile cases, you don't hear much about law firm security breaches. Why is that?**

InfoSec: For one thing, law firms are not subject to the stringent reporting requirements that banks, publicly held companies and retailers must comply with. So rather than damage their reputations and risk losing clients, they don't willingly report intrusions.

212.689.0400

Franchise Technology Risk Management

Our franchise law and computer forensics experts provide consulting and implementation of all aspects of cyber security, ESI management and e-discovery for franchise systems - from preparation of cyber security and ESI-related policies and procedures manuals through collection, preservation, processing, production and presentation.

To inquire about our services, please e-mail
Henry@FTRM.biz
or call (212) 689-0400

We Write the Book

Franchise Regulation and Damages, the only treatise that covers valuations of franchises, is updated 3 times a year.

For more details, to see a Table of Contents or to place an order, go to the Wolters Kluwer Law & Business web page here.

DISCLAIMER

The information provided in this newsletter is for informational purposes only and should not be construed as legal or expert advice which can only be obtained from appropriate professionals. Franchise Valuations, Ltd. and Franchise Technology Risk Management provide such expert advice on the topics addressed herein.

Please visit our websites at
www.FranchiseValuations.com
and
www.ftrm.biz

For another, most firms are not even aware that they have suffered a breach when it happens. They only become aware when they find out that their client's data has been found on a server run by cyber-criminals. Unlike diamond thieves, cyber-thieves operate by copying the valuables, not removing them. So when they are done with their larceny the owners still have possession and don't even know they have been robbed.

And you have to remember that not all threats are external. Another threat vector is the rogue employee, either recruited or placed, acting as a source inside the firm.

***FVR:* What practice areas are being targeted and what are criminals looking for?**

InfoSec: The motherlodes, in terms of information value, are Intellectual Property, Mergers and Tax. If you want trade secrets or licensing agreements, IP is the place to be. M&A has all kinds of information on takeovers and deal terms. Tax departments have all kinds of PII - Personally Identifiable Information - waiting to be scooped up. The same goes for Employee Benefits practices.

A hacking group known as FIN4 has been targeting top corporate executives and law partners who are privy to pending merger transactions and other developments with the potential to move markets.

And in a particularly nefarious twist, FIN4 can command the target executive's email account to delete any incoming messages containing the words "hacked," "phish," "malware," or other words that might warn the user of a potential attack.

***FVR:* I have seen reports that before hiring outside counsel Wall Street banks are pressuring firms to prove they can keep sensitive information secure.**

InfoSec: This is true. Investment banks are upping their due diligence when it comes to hiring law firms. I have seen everything from on-site inspections to questionnaires dealing with security to demands for insurance coverage for data breaches. And if the bank doesn't like your answers, it won't hire you.

***FVR:* Since our readers are from the franchise world, what can you tell us about specific threats they face?**

InfoSec: POS systems are the typical point of entry into franchise systems. Jimmy John's, Dairy Queen, Buffalo Wild Wings and Taco Time were all exposed to cyber attacks in 2014 through vendors of POS systems. The franchise model can make it more difficult for parent organizations to identify and control data breach incidents. For example, in the DQ breach the franchisees had no established process to report data compromises to DQ corporate.

***FVR:* I recently came across a franchise agreement that mandated insurance coverage for data breaches but it's still a rarity. Are you seeing any trends in this area?**

InfoSec: According to a 2014 Ponemon survey, 26 percent of respondents had cyber insurance coverage this year, up from only 10 percent a year ago. They also reported that while awareness of cybercrime is increasing, changes in policy are lagging. Fifty-four percent of companies surveyed reported having privacy and data protection awareness training for employees with access to sensitive personal information. This was an increase from 44 percent in 2013. Companies with data breach response plans in place increased to 73 percent, up from 61 percent last year.

FVR: **What are law firms doing right? What can you recommend as "best practices"?**

InfoSec: There are hundreds of ways to harden your network against data intrusions. If you do an online search, you should prepare to be overwhelmed with suggestions - some cheap and easy to implement, others more expensive and technically challenging. But here are my top picks:

1. **Invest in an audit** by a cybersecurity expert to test and assess your risk of exposure to vulnerabilities, penetration and malware. At a minimum do this a few times a year.

2. **Limit authority to install software** on ANY device that interfaces with the firm network. And don't forget to **change those factory default passwords.**

3. **Conduct continuous employee training.** All it takes is for one employee (or one partner) to respond to a spear-phishing message and the bad guys get in.

4. **Create an Incident Response Plan.** When a breach is discovered, you want to have the people and processes already in place to minimize the damage - Stop the Bleeding - and restore the organization to full functionality.