OAJ Business Torts Section Article January 2016

Law Firm Cyber Breach - To Sue or Be Sued

By: Jim Sammon, Esq.

The 60 Minutes Episode in the early part of this year started with a horrific story about ISIS destroying ancient Christian relics and monuments in Northern Syria. The next segment involved a "War Games" like piece on the incessant Chinese cyber-attacks being launched every second at various large (and not so large) commercial, military, government and industrial targets within the United States. The bombarding of the USA was reminiscent of the final stages of the old video game "Missile Command"; the attacks just kept coming and coming – and in the end – you just run out of missiles to defend yourself – your cities are destroyed and the screen goes black! (I was horrified; terrified; petrified, unable to move. Armageddon was clearly at hand.)

Thankfully, 60 Minutes finished with a touch feely Anderson Cooper playing with cute marine animals. The pain of real life was averted – yet again !

The above scenario happened – and continues to happen every second of every day throughout Ohio. In November 2012, over a million policyholders personal information was compromised when computers at Nationwide insurance and Allied Insurance in Columbus were hacked. 29,050 citizens of Ohio were affected by the Nationwide attack. [i] As a result of the attack, Nationwide provided each affected person with free credit-monitoring and identify theft products.

If you practice in a smaller firm - the seemingly simple solution may be to hide your head in the sand and think "no one would bother hacking into my system – I'm too small." Unfortunately, rather than being off the target radar for hackers – law firms – both giant multinationals and small practitioners are very much the targets of cyber hackers. It is estimated that 80 of the 100 biggest firms in the country have been hacked since 2011. [ii] In a risk-management and control business such as the practice of law – the question becomes "what duty and responsibility do we have to maintain the integrity of the personal information of our clients that is in our possession?" Obviously, the amount and scope of data that is stored by the firm is the foundation of the analysis. But even the smallest of firms may have enough personal information to make them subject to various Ohio laws. Larger firms have an implied duty to pay for the extra ISO Certifications of their websites and intra/internets security systems and settings. What are the duties of the smaller firms – and at what cost?

It has been estimated that a record-breaking 1.1 billion personal and sensitive records were compromised in 2014 across 3,014 incidents. This is a 22.3% increase from the year before. [iii] And this is not just Target or Sony – it is occurring everywhere. Experts report that almost 90% of the data breaches are avoidable. Rather than being the result of high-minded megalomaniac global thieves – many of these thefts simply target smaller companies that have lax security controls. Passwords, user names and email addresses remain the most targeted data types. And as a lawyer, we have a duty to protect not just our client's most intimate secrets – but also their most mundane information.

Ohio's Security Breach Notification laws can be found at Ohio Rev. Code 1347.12; 1349.19; 1349.191 and 192. For purposes of these provisions, "personal information" is confined to an individual's first name, and last name, in combination with and linked to any of the following: social security number; driver's license or state identification number; account number or credit card, in combination with other information that would allow access to the individuals' financial account.

Ohio law mandates any entity that has been hacked to undertake a Risk of Harm Analysis to determine if the client must be Notified of the hacking. The law provides protection to companies and firms if they have taken the steps to encrypt their personal information.[iv] Generally, if the data is encrypted, redacted or altered by technology so that the data elements are unreadable than notification is not required. However, if the breach affects more than 1,000 Ohio residents, than national credit reporting agencies must also be notified. It is these provisions that clearly bring about the duty of even a small law firm to run into an often expensive and potentially complicated notification scenario.

In Ohio, notification is required only if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. Should notification be deemed necessary, it must be provided within the most expedient time possible but no later than 45 days following the discovery or notification of the breach of security (subject to the legitimate concerns of law enforcement). Depending upon the nature of the breach, Notification can take many forms from old fashioned mail to electronic form .[v] Should notification as required under the law not occur, than the offending party could be subject to investigation and a potential civil action brought by the Ohio Attorney General's office.

Much of the litigation in this arena has been undertaken by the FTC through administrative actions against companies for carelessly failing to protect consumer data. The FTC's authority to regulate data breaches as "unfair or deceptive practices" was recently upheld and supported in *FTC v. Wyndham Worldwide Corp*., 2015 US App. LEXIS 14839 (3rd Cir., NJ 2015). The FTC brought suit against Wyndham after three separate cyber-hacking incidents against Wyndham occurred in 2008 and 2009. During those attacks, 619,000 consumers information was compromised leading to over $10.6 million in fraudulent charges. The FTC alleged, in essence, that Wyndham was sloppy and lackadaisical in the application of its cybersecurity practices. Examples included easily guessed passwords; out-of-date operating systems; inadequate restrictions to third party vendors, improper incident reporting procedures and false claims of maintaining an adequate cybersecurity procedure within the hotels.

The *Wyndham* court reaffirmed the right of the FTC to regulate private company's cybersecurity under the unfairness prong. The Court also recognized the FTC's right to regulate inadequate cybersecurity of companies as an unfair (and potentially deceptive) consumer practice. Given the FTC's limited enforcement ability, the *Wyndham* decision opens the door for individual enforcement actions under individual States' unfair and deceptive practices acts. However, given the breadth and size of most consumer breaches, these claims are primarily suited for class litigation. The standing component of individual claimants in such cases is now at the hotbed of litigation throughout the Country.

The moment your firm's electronic information, servers and computers are open to internet or web access begins the time of concern. But even mundane "stand alone" electronics – such as laptops, desktops, phones and tablets can contain sensitive client information that must be protected and is subject to Ohio laws. Should any of these items be stolen or compromised – a Police Report should be immediately made. Many Professional Liability carriers offer both first and third party coverage for a wide range of cyber liability exposures. The addition of this coverage should be explored by any firm who regularly has internet or email communication with its clients. These policies also need to be read and understood by the attorney seeking to assist a potential client who has been harmed as a victim of cyber-hacking.

James P. Sammon, Esq.

12/16/15

---

[i] Columbus Dispatch, December 1, 2012

[ii] Bloomberg Business, March 19, 2015

[iii] Risk Based Security, February 23, 2015 https://www.riskbasedsecurity.com/2015/02/2014-data-breaches-a-billion-exposed-records-a-new-all-time-high/

[iv] ORC 1349.12 and 1349.19

[v] ORC 1349.19(E) (1) through (5)