CULHANE MEADOWS PLLC

Best Lawyers BEST LAW FIRMS U.S.News & World Report 2016

***Kim Verska** is Chief Information Officer, Partner and Chair of the Data Privacy & Security practice of Culhane Meadows PLLC. She can be reached at kverska@culhanemeadows.com or (404) 314-7816 and also tweets @verskette.*

Culhane Meadows (CM) calls itelf "Big Law for the New Economy" and its numerous Fortune 1000 and other client benefit from its innovative business model. All of CM's attorneys are sourced from traditional "Big Law" firms, and have at least 10 years' training, yet CM has eliminated the costly and inefficient parts of traditional law firms including dedicated office space, associates, secretaries, marketing or other non-necessary administrative personnel.

Note: the following is offered as general recommendations and observations by the author and does not constitute legal advice to any company or person, or constitute a representation by the author or CM of any company or person. For specific legal advice for your situation, please contact the author directly as noted above.

The Legal Side of Data Breach

1. **Top Three Takeaways from Legal Perspective**
    a. Your Nightmare is a Plaintiff's Lawyer's Dream
    b. Play Out the Serious Breach Nightmare Scenario NOW
    c. Ounce of Prevention (Encrypt! Encrypt!)
2. **Your Nightmare is a Plaintiff's Lawyer's Dream**
    a. Legal Actions On the Rise. A consumer data breach will automatically mean one or more lawsuits or government proceedings these days, due to a confluence of factors.
    b. Expenses for Victims = Ticket to a Successful Class Action. If you have a breach, ***DO NOT*** let your victims come out of pocket – the answer is "let us help protect you/fix it, ***FOR FREE***"
        i. Damages like out-of-pocket expenses are usually the biggest hurdle to class action payouts in this area
        ii. If you have reason to believe victims have more serious problem, consider what you would think was a **reasonable way** to "make it right" for your customers
        iii. Pay for identity theft protection from major credit bureau or similar to protection to what similar companies have done
3. **Play Out Serious Breach Nightmare Scenario NOW**
    a. Play "Let's Pretend" With a Privacy Lawyer. You need to understand the main things the Federal Trade Commission (or a jury) would be looking at if you have a breach. This can be a one-hour consult – **far better than the ostrich approach**.
        i. Imagine **that you can keep nothing secret** – how will it look on the front page of the Wall Street Journal?

ii. The watchword in a legal action is whether what you did to prevent and to react to a breach was **reasonable**. What would be the prudent and reasonable steps to take in light of the biggest risks to your customers?
iii. The **perfect is the enemy of the good**: figure out the biggest risks, write a DIY security plan dealing with those, and implement it as best you can
iv. Again, spend a small amount of money with a privacy lawyer/expert to create a **list of must-haves** so that you can say with a straight face "we took reasonable steps." For most, these will include:

1. Procedure for complaint handling – "red carpet treatment"
2. Procedure for data breach – (see Item 5 below)
3. Data inventory and sensitivity review
4. Data security policy
5. Review of contractors to comply with above
6. Training for key personnel

4. **An Ounce of Prevention (Encrypt! Encrypt!)**. These are things to do now, to knock out the biggest "If only…" factors that breached companies later reflect on.

a. Watch the news and **apply key patches immediately** (over 3 months' unnecessary vulnerability to Heartbleed created **in the majority** of VMWare users: http://www.securityweek.com/organizations-slow-patching-heartbleed-vmware-deployments-report)
b. **Encrypt all sensitive data** in transmission and storage (cost of each lost piece of sensitive PII in 2015: $154 http://www-03.ibm.com/security/data-breach/)
c. **Beware all eggs in one basket**, even if it's the Amazon Web Service Cloud (Exhibit A: Code Spaces, now out of business http://www.networkworld.com/article/2366862/iaas/a-wakeup-call-for-the-cloud.html)
d. Warn all employees, **watch unhappy employees** – FBI reports this is on the rise (http://www.techinsurance.com/blog/cloud-security/fbi-reports-more-data-breaches-from-disgruntled-employees/)
e. Force password strength and change, and **fight stupid passwords!** – print out all employee passwords and if any of these are on the list, ding that person's annual evaluation: http://www.someecards.com/entertainment/web/the-25-most-commonly-stolen-passwords-stupid-people-were-still-using-in-2014/
f. If the above is not being done, apply mobile device security software or similar

5. **Current Trends**

a. Private litigation and state enforcement based on "failure to adopt reasonable security measures" under unfair/abusive trade practices regimes, especially for PCI breaches; amounts of fines going up (2015 AT&T case $25MM, but larger amounts in state AG actions)

b. Types of breaches – hacks are on the rise; accidents and "portable device loss" and similar are falling. Good overall resource at http://www.privacyrights.org/data-breach/new

c. Companies getting in trouble due to their service providers (2 FTC cases in 2014 for failure to verify procedures/allowing unneeded access to PII)

d. Proliferation and changes in "data breach" laws with specific requirements

i. Mass Regulations are the standard for encryption: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
ii. Some states breaking away from traditional definition of "protected personal information," shortening the notice period to 30 days, adding other requirements. FL is best model here:

http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

iii. WA's 2010 law regarding PCI compliance follows in footsteps of those of MN and NV first ones: http://apps.leg.wa.gov/Rcw/default.aspx?cite=19.255.010

iv. Call for federal legislation,

v. U's new law effective in 2017 has damages of "4% of the breaching entity's worldwide revenues"

e. Next shoe to drop: successful certification of class actions (need some out-of-pocket expenses across class and/or "imminent future harm" as per Neiman Marcus 2015 case)

6. **Procedure for Security Breach**. Assemble (a) and (b) ***this month***. Then, if the worst appears to have happened, do the following:

a. Identify/convene key internal team (commitment to drop everything else)

b. Identify/convene key external team (privacy attorney and forensic consultant (just in case))

c. Once a loss/intrusion has been determined probable:

i. Stop the presses! Change passwords, freeze system in question, stop further data movement. Do not allow document destruction, even under regular document destruction policies.

ii. Careful not to compound the problem: once you see a consumer's data has likely been compromised, be sure consumer has no out of pocket damages (this was one mistake in Target).

iii. Assess your actual data loss, types of data, and residents of which states have been impacted – need experienced data privacy lawyer.

iv. Contact a "data breach notice provider" to provide your notices (you do not want to DIY or the wrong kind of data privacy lawyer for this).

v. Watch your mouth! Top execs can compound the problem. You may need a PR expert.

d. Document what happened, upgrade something or make notable change, document the changes you have introduced.

CULHANE MEADOWS PLLC

BIG LAW FOR THE NEW ECONOMY™