WINTER 2014 E-NEWSLETTER

I SEE DEAD PEOPLE
MANAGING THE DIGITAL GRAVEYARD

Ever receive a Facebook message or a tweet from a deceased family member promoting some diet and weight loss program? So have we at **Digital Mountain**. Which made us think about how both the living and their heirs need to worry about social re-engineering. Just as we have wills, trusts and healthcare directives, we should have digital account directives.

With Facebook's approximately 1.2 billion -- and rapidly growing -- users, the social networking graveyard problem has just reached its infancy. According to the CIA World Factbook, as of July 2013, there were approximately 7,095,217,980 people on the planet and the death rate was approximately 7.9 deaths per 1,000 people a year (equating to roughly 56,052,222 deaths each year). Using these metrics, about 7.9% of Facebook's users may become part of the digital graveyard within 10 years. Without replenishing users, within 60 years, there may be more profiles of the deceased than the living. This means Facebook potentially has over a million accounts to de-activate or delete every year.

Perhaps we have a new field coming our way for those in the IT and legal industries?

THROWING DOLLARS AT THE DE-NIST PROCESS

The de-NIST process is used by many push-button e-discovery vendors for excluding system and application files based on the NIST National Software Reference Library database of approximately 19 million unique file signatures. Hash values or digital fingerprints of files are compared to the database and excluded if they match.

The problem with this approach is computers make a high number of extraneous files after system and program files are installed, so this may catch a large volume of junk files such as bookmarks, cookies and other files created by ordinary computer usage, but not necessarily considered user-created files. Additionally, system and/or application files not on the NIST list may be included. Assuming 40% of 100GB is program and system files from a hard drive, and a vendor charges $100/GB-$200/GB for de-duplication/keyword searching and date range filtering, this may result in $4,000-$8,000 of extra costs due to having a push-button technician with little understanding of underlying data being

processed. So although your vendor may have really inexpensive GB pricing, the total cost of processing may end up ultimately being higher.

Although **Digital Mountain** will de-NIST if the customer requires it, we strongly recommend having a data expert analyze the drive based on the underlying file system. Utilizing a forensic program, the expert will assess where user-created data and email resides. This is typically performed on an hourly-based model of $250 to $400 depending on the vendor. The median analysis for user-created files and email may range from 1 - 1.5 hours resulting in optimal results without the junk that you still get in the de-NIST process. This process provides the added savings of attorney review time and better quality results. The caution is the vendor must have data experts and not just low level technicians who used to print paper and now follow a step-by-step process outlined on a wall.

It's important to question the methodology and not just seek the lowest price per GB unit, so you end up minimizing total costs and maximizing value for your organization. ***Contact us at 866.DIG.DOCS or info@digitalmountain.com to work with our experts.***

DIGITAL MOUNTAIN'S GUEST CONTRIBUTOR
DAN LUNGREN

As the former Congressional House Chairman on Cybersecurity, a subcommittee of the Homeland Security Committee, cyber security is a topic in which I continue to be deeply involved.

The cyber world is ubiquitous, directly affecting each of us in personal and global ways, yet it is little understood or appreciated; as a result, the nature of cyber threats, from the mundane to the critically serious, are ignored or given insufficient attention. The threat needs to be addressed by all, but particularly companies needing to protect their intellectual property, privacy and security.

The recent security breach at Target should serve as a wake-up call for many. In addition to the loss of private information for as many as 70 million individuals, the evident breach has serious, real consequences for the companies involved. Already there have been indications that a number of investigations on the federal and state levels are imminent. Additionally, there is the specter of private litigation on behalf of those individuals negatively affected. Finally, there is the adverse impact on consumer confidence.

Those who seek to hack into, and or otherwise disrupt, the various elements of e-commerce are nearly unlimited in number - both in terms of their identities and their unique approaches - making it impossible to mount a perfect or failsafe defense.

So what to do? What is the appropriate stance for companies situated such as Target? Obviously doing nothing is not the answer. Defense and mitigation strategies must be established and implemented. The fact is that there are many approaches available. At a minimum, a comprehensive program is necessary, starting with a company culture of good computer hygiene extending all the way to a robust cyber security regimen endorsed and enforced at the highest corporate levels. In today's environment, cyber security must be part of a company's DNA.

But then how to judge how much protection is enough? And whose protected interests are paramount?

While the final answers are likely to be played out in many different venues, the resolution of the matter should center on whether the company faithfully followed the contemporary industry standards for protecting their clients'/customers' confidential information. Here, the challenge is how to appropriately and fairly ascertain such standards.

Some suggest that this should be a product of happenstance - allowing the underlying legal

standard to be determined by many individual judges or juries in the context of active and endless litigation. Others argue that the determination should be made by the various state legislatures. I would argue that such uncertainty is neither in the interest of the ultimate consumers nor the companies involved. It is for this reason that I continue to argue for legislation on the federal level that would accommodate the twin necessities of market dynamism and legal certainty implicated in a deft regulatory scheme. As envisioned, voluntary industry standards developed with the cooperation of the private and public sectors, would, if followed, afford certain legal immunities. Such standards would be performance-based rather than prescriptive and would necessarily bring the insurance industry to bear on the equation.

These, and many other questions, have been raised and discussed at meetings and conferences throughout the United States, and abroad. In November, I participated in two such conferences, one hosted by the University of Notre Dame Law School and another by the University of Pennsylvania. These types of conferences, along with many other organizations, bring together cyber security thought-leaders for enhancing guidelines and preemptive procedures for data protection.

- Dan Lungren

The Honorable Daniel E. Lungren served in the United States Congress from 1979-1989 and 2005-2013. He was California Attorney General from 1991-1999. Congressman Lungren is a lawyer, national speaker and media commentator on such topics as immigration, law, and cyber security. He can be contacted at linkedin.com/in/danlungren.

To work with one of Digital Mountain's cyber security experts to address your company's data protection plan, contact us at 866.DIG.DOCS or info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

January
ALA Midwinter Meeting: January 24 - 28

February
LegalTech New York: February 4 - 6
The Sedona Conference® Cooperation Training Program: February 12 - 13
RSA Conference: February 24 - 28

Click here to see more upcoming events and weblinks

DIGITAL MOUNTAIN, INC.
5050 El Camino Real, Suite 205
Los Altos, CA 94022
866.DIG.DOCS

Contact us today!

www.digitalmountain.com