SPRING 2014 E-NEWSLETTER

At Digital Mountain we assist our clients with their cyber security, e-discovery and computer forensics needs. With the recent data security breaches making headlines, and affecting millions, we chose to theme our Spring 2014 E-Newsletter on how to protect your personal and professional data.

DIGITAL MOUNTAIN'S GUEST CONTRIBUTOR
ERIC P. MANDEL

A BROADER VIEW OF INFORMATION SECURITY

"In trying to defend everything he defended nothing."
Frederick II of Prussia (Frederick the Great)

Information is the lifeblood of modern business. Through the information it gathers, analyzes, and acts on, an enterprise can recruit and support a labor force, locate clients or customers, and develop and deliver innovative products and services.

Information assets are well worth maintaining, but there are real-world risks and costs in doing so. The use of data security programs to prevent loss of information is the focus of many in the tech business. If you're reading this, you've likely already heard the horror stories of data breaches, trade secrets copied by competitors and foreign actors, banking, financial and credit records being hacked and sold online in huge batches, and employees carelessly leaving open back doors to the most highly secured networks by clicking on an email link.

The loss of information, particularly in the form of data, is a real risk. It is something faced by governments, businesses, educational and non-profit institutions, and individuals. Organizations impacted by data breaches in the last decade span the spectrum of industries. The number of incidents is rising, and there is no organization too big or too small to become a victim. A May 2013 report from the Ponemon Institute indicates that US companies are incurring, on average, $188 per affected user, which when multiplied can quickly add up to significant sums.

The source of a data loss may be intentional malfeasance of hackers or inside actors, whose motivations can range from financial gain (e.g., credit card fraud), to industrial or governmental espionage to global and personal activism (e.g., Anonymous or revenge porn). But information loss may also occur from unintentional or ill-conceived actions by a poorly trained or careless individual, or from technology or process errors.

Regardless of source or motivation (if any), the results of a data loss can be devastating to an organization’s reputation, financial well-being, or both. A patchwork of federal and state laws and regulations in the United States impose requirements for protecting specific types of personal information, and penalties for failing to do so properly. If personal information is released in significant numbers as the result of a data loss, 46 states have requirements for notification to affected individuals. Further, an enterprise that tells the public that it protects the personal information in its possession, but fails to reasonably do so, may be subject to hefty fines from the Federal Trade Commission.

It may seem obvious that the best protection against the consequences of a data loss is for an organization to implement effective defensive measures to protect against risk across the spectrum. Some organizations have spent small fortunes to lock down data systems and protect against malicious and careless actors inside and out. While aggressive programs can be put in place to seek out and purge data, particularly email, to ensure it will not land in enemy hands, such programs can easily fall into the adage that to defend everything is to defend nothing.

When I was a child, my home was robbed, and my mother's engagement ring was stolen. The result was that for many years, if there was going to be a dinner party or an evening out with my father, my mother would have to go to the bank to get her jewels from the deposit box. This kept the jewels safe, but it also kept them from being worn. Over time, some jewels – those that were less expensive or could be more easily replaced – were left at home, and only a select few were kept in the safe.

Jewelry should be worn to display its beauty, not stored in a vault. Likewise, information should be leveraged to maximize its value to the organization. Data security should not be designed so inflexibly that it prevents the organization from obtaining value from the information it seeks to protect, nor should employees be prevented from doing their work by having to jump through impossible hoops in the name of security.

There must be a balance struck between information security and information access. So, when developing a defensive but functional program, consider the following:

First, there are multiple stakeholders involved with the creation, use, and defense of information and the associated risks and costs. This may be, in some organizations, a core consideration of corporate governance. The needs and interests of all key stakeholders should be considered, and balance should be sought when needs and interests are in conflict.

Second, not all information is the same. There are differing degrees of value, risk, obligations, and security. A properly designed information program will classify information created by or entering the organization to determine a variety of key factors, including (a) the known or potential value of the information, (b) the risks and obligations associated with retaining and using or repurposing the information, (c) the risks and obligations associated with disposing that information, and (d) the appropriate level of security that should be applied to that information in retention, transmittal, and eventual disposition. The key risks and obligations that should be considered include legal issues, regulatory compliance, and privacy.

Third, it is useful to understand the costs associated with retaining information, as well as the cost of locating, reviewing and providing that information in response to legal or regulatory discovery obligations.

Fourth, keeping in mind the admonition of Frederick the Great to avoid trying to defend everything, employ a combination of reasonable and appropriate technologies and policies, including monitoring systems, to help reduce the probability of data loss through malfeasance and carelessness. Policy development should balance the stakeholder needs noted above, as well as technical and human requirements, including employment law considerations.

Fifth, accept that at some point information that should have been protected will get out in the wild. Develop, and from time to time update, a response plan that addresses what the organization will do when that occurs. There are 46 different data breach notification laws in 46 states related to the release of personal information. Some of them have relatively short timelines for the notification to go out before fines start stacking up that will dwarf the cost of pre-planning, which alone should be sufficient motivation for the creation of a response plan.

Sixth, consider insurance coverage to mitigate and transfer some of the costs associated with risk of data breach, property damage, business interruption, brand injury, and related risks.

Ultimately, taking a more comprehensive view of information – and its value, risks and costs – is the key to implementing and maintaining a balanced and appropriate data and information security program.

Eric P. Mandel leads the E-Discovery and Information Governance practice at Zelle Hofmann Voelbel & Mason LLP. As an attorney, legal technologist, and well-recognized industry thought leader, Eric serves on multiple industry policy and standards setting bodies, including the Steering Committee of The Sedona Conference, Working Group 1 (WG1), and the Advisory Board of Electronic Discovery Reference Model (EDRM) trade group. He is also a member of the International Association of Privacy Professionals. Eric is admitted in California.

If you would like to be considered as a future Guest Contributor to a Digital Mountain E-Newsletter, please provide a biography and a description of the proposed article to marketing@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

April

EDRM 2014-2015 Kickoff Meeting: April 22 - 24

ACEDS 2014 E-Discovery Conference & Exhibition: April 27 - 29

May

E-Discovery 2014 National Institute: May 15 - 16

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

Know someone looking for work in the e-discovery, computer forensics and cyber security industries, with entrepreneurial characteristics? If so, please share this great job opportunity with them: Seeking a Business Development Associate to join our energetic team. ***Read more...***

DIGITAL MOUNTAIN, INC.

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

www.digitalmountain.com

Contact us today!

FOLLOW US AT:

in f