DIGITAL MOUNTAIN®

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 and digital assets.

HOW ARE YOU PROTECTING YOUR CUSTOMERS' AND YOUR ORGANIZATION'S DATA?

With the recent Target, Neiman Marcus and Adobe Systems data breaches, coupled with the Heartbleed bug exposing OpenSSL for many mainstream Web-based email accounts to hacking, cloud information security is now more important than ever. Additionally, data breaches at law firms such as Wiley Rein, among others, have organizations on high alert to be reassured that their sensitive information will not only be secure in-house, but also at their representing law firms and at the vendors handling and hosting their data. *At Digital Mountain we continue to make this a top priority.* A number of our law firm clients now have an attorney at the partner level spearheading their Cyber Security practices. Also as a reaction to data security concerns, groups such as the Cloud Security Alliance, ILTA's LegalSEC and the Sedona Conference on Cyber Liability have formed. With all of the information out there, we are repeatedly asked by our clients to identify laws, guidelines and certifications with which to comply. So we created the below list.

Government entities have created certifications, guidelines and laws for organizations to follow such as the US-EU Safe Harbor program for data from the European Union and US FedRAMP. One such law is the Health Information Technology for Economic and Clinical Health (HITECH) act. The HITECH act coincides with the Health Insurance Portability and Accountability Act (HIPAA) as the privacy and security portion of the law and how it deals with digitally stored media. The HITECH Act extended the reach of the HIPAA Privacy and Security to include Business Associates such as law firms and vendors. Under the HITECH Act, business associates are now directly responsible since they are required to comply with the safeguards contained in HIPAA. What this means is that U.S. Department Health and Human Services will enforce and prosecute any infractions relating to protected health information such as data breaches. Furthermore, organizations that do not follow these government guidelines cannot do business with entities in their respective regions. Therefore, it is imperative that your organization's cloud security is up to date. A way to make sure of that is to be certified.

Here are certificate programs or frameworks to consider:

1. **The ISO/IEC 27001:2005** information security standard requires that firm or company management assess the current information security risks, design and implement information

security controls to address those risks and adopt an organization-wide information security management process to make sure that the security controls continue to meet the organization's information security needs as time goes on. To be certified, your organization must implement the aforementioned steps through an information security management system and have that system audited regularly by an accredited auditing body or registrar. This certificate program is the basis for the next certificate program as it deals directly with access control and asset management.

2. **The Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)** is based on having an independent auditor assess the current information security system much like the ISO/IEC 27001:2005 and then to be added to the registry. The organization must also have ISO/IEC 27001:2005 before embarking on STAR. Once the organization has achieved ISO/IEC 27001:2005, the first step in the STAR certification process is to do a self-assessment through submitting either the Consensus Assessments Initiative Questionnaire (CAIQ) or the Cloud Controls Matrix (CCM). The CCM is then used as a guideline addressing any shortcomings with current information security policies. Once the organization is in compliance with ISO/IEC 27001:2005 and the CCM, an independent auditor will test and score how well the organization adheres to guidelines with certification reached by being listed in the registry as STAR Certified.

3. **The Statement on Auditing Standards #70 (SAS 70) and its successor, the Statement on Standards for Attestation Engagements #16 (SSAE 16)** are not certificates, but are standards illustrating that organizations have defined processes for reporting on controls. Firm or company management would write written assertions and that independent auditors would verify those written assertions. This is primarily useful for service organizations to show that their current systems have been audited and will eventually build trust with the organization's customers.

4. **The US-EU Safe Harbor program** is a framework in response to the European Commission's Directive on Data Protection which enables US-based organizations to do self-certification based on the Safe Harbor principles of Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement. Although the Safe Harbor program is voluntary, it is beneficial for US-based organizations to join the program because all 28 member states of the EU are bound by the European Commission's standard of adequate data security standards and thereby streamlining the process of working with other organizations based in the European Union.

5. **The US Federal Risk and Authorization Program (FedRAMP)** is a certification program that enables organizations to provide cloud services to the various U.S. government agencies provided it passes the two step process. The first step is a security assessment based on NIST/FISMA guidelines; once a third-party assessor determines an organization's compliance with FedRAMP baseline controls, it is granted provisional authorization by the Joint Authorization Board comprised of the Department of Homeland Security, Department of Defense and the General Services Administration.

Beyond laws and certifications, there are many guidelines and checklists that corporations and law firms should be aware of including NIST's Computer Security Incident Handling Guide, SANS Institute's Incident Response Forms, The ABA Cybersecurity Handbook and Digital Mountain's data security questionnaires. There are also a growing number of data security and privacy conferences, which are tracked at Digital Mountain at: http://www.digitalmountain.com/events.

To learn how to better protect your organization or to respond to a data breach, please contact us at at 866.DIG.DOCS or info@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 🐦