Management Innovation: Technology
MassHousing – Securing Private Information: The HFA That Keeps The Secrets

Overview

The effective compilation of consumer information is the backbone of MassHousing's – and indeed every HFA's business processes. Much of this information is private personal information, entrusted to MassHousing by consumers as they describe their financial circumstances sufficiently for us to make lending and/or rental assistance decisions.

Ensuring the confidentiality of that private personal information is critical not only to earn the trust of the Agency's clients and business partners but also to protect the Agency from the liability that a security breach would bring. Unfortunately within the current electronic communications environment lurk vulnerabilities that may compromise personal information held by the Agency.

Every day there are stories in the news about security breaches involving personal information including social security numbers, bank account numbers and license numbers. These events wreak havoc with the personal credit history of their victims, destroy consumer confidence in even the most trusted institutions and cause considerable damage to business reputations. Incidents of data breaches of personally identifying information totaled 653 world-wide in 2008, affecting over 84 million personal records. Over the past five years, more than 1,600 breaches have occurred in the U.S, representing exposure of 270 million protected information records. Some particularly unfortunate victims have even experienced multiple incidents! As consumers grow more wary of this threat, government is reacting with new legislation to ensure that those entrusted with private personal information meet higher standards for security to ensure its protection.

For businesses, the cost of dealing with a data breach includes detection, notification, response, and lost business. According to a 2008 study of the Ponemon Institute, the average data breach cost of one lost laptop in the financial services industry is $68,862. The average cost of repairing a breach of 10,000 records is $2 million. A total of 88% of cases in the Poneman Institute's study involved insider negligence and 35% involved mobile data-bearing devices like laptops and PDAs.

From the victim's standpoint, reconstructing one's credit after a data breach is costly and time consuming – and can range from as little as $30 to thousands of dollars. Most importantly though, a security breach disrupts a victim's ability to conduct his or her daily life. Obviously, this is something MassHousing will work hard to avoid for its customers.

MassHousing's Approach

1. Early Implementation

MassHousing takes its responsibility for securing personal information very seriously. As early as 2003, the Agency created a written Information Security Program (ISP). MassHousing's ISP implemented policy and procedures consistent with the requirements of the Graham-Leach Bliley Act. First, it defined Non-Public Personal Information (NPI) and established management and IT procedures designed to enhance the protection of such information, principally social security numbers. The ISP also established Privacy Officers within each of the business lines and mandated the use of strong passwords (passwords too complex to be discovered by computer programs or cyber criminals) by all Agency personnel. These changes laid a strong foundation for the Agency's privacy policies.

In 2005, recognizing the importance of ensuring that only authorized users could access MassHousing's systems, the Agency began installing fingerprint scanners on all PCs. Now every authorized user places their finger on a scanner anytime a password is required. This one device increased security and ease of use at the same time, since users merely have to swipe their finger instead of keying an eight or more character password. In fact, temporary workers are issued very long and complex passwords which are never revealed to the individual. For these workers, only their finger scan will grant access thus ensuring that passwords cannot be shared.

2. *Increasing Federal and State Requirements*

Since the initial formulation of our ISP, a number of laws have placed additional requirements on MassHousing. Some of these laws have been at the Federal level – 2004 FACT Act (15 U.S.C. § 1681) and Federal Trade Commission at 16 C.F.R. Part 314 – and others have been enacted at the state level. In 2008, the Massachusetts Legislature passed a law and then published standards for the protection of Personal Information of Residents of the Commonwealth (M.G.L. Chapter 93H and corresponding regulatory standards contained in 201 CMR 17.00).

The Massachusetts Law is the most stringent of any state's privacy legislation – it expanded the list of personal information to be protected, creating a definition of Protected Information (PI) and specified that every person or business that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits this information must have a comprehensive written Information Security Program (ISP). The law's intent is to ensure the security and confidentiality of personal information and protect commonwealth residents against unauthorized access to or use of their PI which could result in substantial harm or inconvenience. Massachusetts's new requirements are now seen by many industry watchers as the standard for future action by other state legislatures.

In response to the law, MassHousing first updated its written ISP. During the review of the written policy, the Agency expanded the definition of protected information. This meant going beyond social security numbers to include such things as names and a corresponding Massachusetts drivers' license number, or a financial account number or credit card number.

The Agency also needed to understand all of the sources of PI within the Agency's files so that it could be protected most effectively. As a result, IT staff surveyed systems for the location of PI stored in both files and databases. PI was found everywhere – in MassHousing's data center databases, on shared drives, PCs, phone system voicemail, mobile workers' portable devices, on the open internet as MassHousing conducted business with consumers and business partners and when employees accessed Agency files from remote locations. The scope was enormous.

The Agency contracted with an external professional information security firm to conduct an independent assessment of MassHousing's Security Policy, IT infrastructure and operational procedures. The company's review revealed both real as well as potential information security threats and made recommendations to correct the areas where breaches could possibly occur. The Agency then established a plan to implement recommendations based on the requirements of the new law and the findings of the information security firm – all within the deadlines required by the new state law.

To start, MassHousing needed to re-establish information security as everyone's responsibility – the receptionist who greets consumers making a mortgage payment – the mail clerk – a loan officer – and even the Executive Director. The Agency's user access policy was revamped so that each user's data access permissions are aligned with their job role – ensuring their access is consistent with a "need to know" to perform only the functions of their specific job. All information stored on laptops and backup media was encrypted, and disaster plans were modified so that it could be decrypted in the event of its need for disaster recovery. An encrypted email service was provided for all users – allowing them the ability to share PI securely. Additionally, MassHousing enhanced its requirements for background checks for all new employees and temporary workers who are granted access to MassHousing systems. Additionally, the role of MassHousing's newly established Privacy Officers was redefined and these individuals were trained in their responsibilities.

3. Training and Intra-Agency Coordination

For the Agency's efforts to be successful all Agency staff had to fully understand how to recognize PI and to understand the importance of their role in protecting this information. Security awareness training course materials were created and used to train all users (employees, temporary workers, interns and contractors). The most important aspect of the training was to understand when it is appropriate to share PI and how to do it property so that security is preserved. Additionally, a Vendor Confidentiality Contract Addendum was developed and all contract workers or businesses that will come in contact with PI are required to agree to protect it.

Finally, a process was needed to ensure alignment between legal and business requirements on an on-going basis. An ISP Task Force was formed, and included the Directors of IT, Administration, Internal Audit and a Legal Staff member. Initially, the Task Force guided the development of policy and procedures consistent with legal compliance and business needs. Now, the Task Force will authorize additional measures including further encryption for PDAs, CDs/DVDs, USB drives and will also set policy going forward so MassHousing is compliant with current law as it evolves and remains ever vigilant for future threats.

Conclusion

MassHousing has made major strides in increasing the security of the protected information entrusted to the Agency in the course its business. In 2004, CIO Magazine named MassHousing one of the 100 most "technologically agile" companies in America. The Agency believes that is as true today as it was five years ago, and we continue to use technology and management practices to respond to the ever-changing business environment in which MassHousing participates.

We are eager to spread the word to all HFAs about the importance of securing PI. We have shared our experience with the NCSHA Membership during presentations at the last three NCSHA conferences and we have made our ISP documentation and training materials available to the membership for their use.