Identity Theft prevention in Legal Plans and Healthcare Reform

The drive to streamline service and to provide employees and more people with access to legal plans and healthcare has led to some great gains in the provider structure. It has also created what could turn out to be a golden opportunity for wide scale identity theft. The various healthcare reforms coming into place with the Affordable Care Act, the new ISD 10 and electronic health care records (EHR) protocols promise to provide a portable and consistent means for treatment. The legal plans offered by many companies to provide for affordable legal services are following the design of using electronic databases to coordinate service and to maintain member information. All of this means that sensitive and confidential information is stored electronically and that can leave it open to theft. The real question is whether or not all of these new systems are being rolled out before adequate testing of their security has been done. If the past few months of the healthcare reform enrollment are any indication, the answer is no. The question that then follows is whether these systems have allowances to repair themselves or are members faced with constant Band-Aid patches only after a new security flaw has been revealed.

Why would these programs be released with such tremendous security flaws?

The unfortunate standard of the data and software industry is to rush a product onto the market before it is thoroughly tested. The 80s were the last time consumers had to wait through closed beta testing periods before a version was released to the general public that may not have been perfect, but it had most of the major bugs discovered. The problem with this protocol is that it was expensive and time consuming. As the software industry picked up its pace and began to play for big money, the idea of contracting with outside test groups for months on end before a release was deemed economically unsustainable. Developers began to rely on consumer complaints to find the bugs that would have been found under the old testing process. As more and more systems came online such as healthcare, finance and legal databases and services, the amount of confidential information stored increased. This gave rise to the Black Hat Hacker who would break in to steal the information for sale to criminal enterprises. Identity theft became a very real reality for the average consumer. While software companies didn't change their release procedures to combat this, a new profession has risen – that of the White Hat Hacker that is serving to help find some of the greatest loopholes in new systems before the criminals do. White Hat Hackers are computer programmers who deliberately try to find the weaknesses in a program that would allow them to steal mass identities, but they report the issue rather than take advantage of it. They are compensated on a reward basis by most companies. At least that is how the industry usually treats a White Hat that arrives to save the day.

Under a White Hat – When help arrives for a problem no one wants

When the Affordable Care Act rolled out its enrollment websites, problems were everywhere. The sites didn't work, people couldn't sign up (but a Bichon Frise in Texas had no problem) and it was generally considered to be a disaster. It wasn't that there were obvious security loopholes; it was that the whole website and database systems didn't work at all. While Washington was busy pointing fingers and throwing blame around, a few White Hats were trying to sign up for healthcare; Kristian Erik Hermansen was one of them. Hermansen makes his living as a professional White Hat, working for a data security firm in L.A. that is hired to try and break into systems to find weaknesses before a criminal does. No one hired Hermansen to poke at the Healthcare site; he just noticed what seemed to be very obvious open doors. It didn't take long for him to figure out how to get in; not just to someone's indiviudal account, but to the admin control which would have let him take 100s of identities. When he tried reporting his findings to the site administrators, he was ignored. When he tried calling them, he was ignored. Not until he posted a YouTube video detailing the loophole did the government pay attention to him. Even then, they were more concerned about stopping him from talking about it then talking to him to find out the specifics. Hermansen has noted that several months after the FBI showed up telling him to stop – the loopholes have been fixed.

Do all group plans create security problems?

While it could be argued that anytime a service is based upon a database of confidential information there is a high potential for identity theft, but that doesn't accurately portray the problem or the possible solutions. With the growing trend towards legal plans, the information hosted on a server in a group membership for an employer or as a service plan is going to contain even more critical information than just enough to allow someone to steal an identity. Identity theft right now is limited mostly to social security, passwords and account numbers; should the information taken also include medical history, next of kin, assets and holdings the destructive potential is immeasurable. Not all group data plans need to be at risk. Key to creating a safer environment for data is not to move it offline or limit what is stored, but to change the culture of development and response.

Working to change the culture of development and response

The current culture of development and response to security breaches and loopholes is a direct result of the "done yesterday" approach to bringing databases and systems on line. Decades ago there was the beginning of a discussion about creating a standard for release of databases that were exposed to the Internet that treated their approval much the same way a new medication is processed before being made available to the public. The groundwork for changing the thinking and style of development is aided by the language used in describing the security issues software and databases face. Programs aren't broken into, they get viruses and machines are infected. If the approach to development is directed away from speed of production when the information that will be held is of a critical nature, much of the security issues present today will fall by the way side. The problem can't be resolved by just slowing down the process, more emphasis and investment has to be put into developing technology and computer engineering education initiatives.

Developing programmers who can create

In the rush to fill jobs quickly, most of the computer industry has come to prefer a "cut and paste" style to adding code to create larger projects. Without proprietary code, programmers who know how to author from scratch and departments that have the time to create programs – there will always be loopholes in security that can be exploited. While much of the rest of the world is leaping to fund technology education initiatives, the US is cutting funds. To be cutting funding to an industry that is now expected to manage the confidential data of a nation is nothing short of begging for a massive theft of identity. Since the “cut and paste” style is so necessary to meet designs for database development. Back hat hackers know that if they are patient, they will be able to find a loophole they already know how to exploit in almost any secure database.

What is the best means to protect against identity theft?

In the meantime, how safe can legal plans and health care reform data be? It is going to take a new level of accountability and watchmanship to make sure that the confidential information stored on servers remains secure. More checks and balances need to be put into place and that includes checks and balances on the consumer side as well. It is no longer responsible for anyone registered for any type of plan, legal or health, to rely upon system alerts to notify them of identity theft. Consumers should be educated on how to check the information and activity on their account on a monthly basis to help spot discrepancies sooner. Companies charged with managing data also have to develop systems to spot the fake accounts that are used by Black and White Hats to test the security of a system. Hermansen’s first discovery about healthcare.gov being simple to break into an individual account has been discounted far too quickly. While simply breaking into a user account will rarely let you see their full social security number, it does give you enough information to begin to process fraudulent claims. Keeping a sharper eye on the front and back door of the system is the only way to keep consumer data safe while new standards of development and testing are adopted throughout the industry.