TRIAD BIOMETRICS®

September 16, 2010

With respect to quantifying the economic impact of PII breaches, evaluating authentication / ID management, fostering global engagement, and providing an incentives framework for evolving cyber-risk options and cyber security best practices, Triad Biometrics LLC makes the following comments:

Quantifying the economic impact. Quantification of economic impact resultant from data breaches is nebulous; however, some observations can be made from the standpoint of the entity administering the database, the specific victims whose data is breached, and society as a whole. For the administering entity, quantification of damages can be related to direct economic impact suffered by them such as reduction of equity valuation as a result of publicity associated with a breach. For example, a public company with a market capitalization of $ 1 billion that suffers a 10% decline in its stock price as a result of a breach associated with a breach experiences a $100 million reduction in perceived and actual value. Reputational damage becomes monetary damage. Direct expenses associated with a breach also include legal expenses defending against suits, settlements and judgments of such suits, and fines levied by various statues. All these direct expenses have easily quantified economic impact. Quantification becomes more difficult when addressing the victim whose data has been breached. Clearly, the contents of the breached data here are key as not all information has the same value. Data giving criminals access to bank account balances do not have the same value as access to a social website. Quantification in the case of bank account breaches can be quantified by a parabolic function whose value declines more rapidly as time passes because, over time, defensive actions can be taken to reduce the potential value of the data (closing breached bank accounts for example). In the case of irrelevant personal information, quantification is immaterial. From a societal standpoint, economic impact can be pervasive for breaches that have direct economic impact as such breaches will erode confidence of the populous in the internet and, as a consequence, economic activity both on and off the internet as breaches of PII often directly lead to increased incidence of impersonation and identity theft of individuals. To project such economic impact is very difficult if not impossible other than to estimate that the multiplier effect would be diminished by some amount related to the economic value of the breach. It appears that categories of breach targets could be compartmentalized, and then fines could be levied for various infractions and levels of breaches of data that were inadequately protected by entities maintaining the database. Quality levels of protection would have to be established that would adjust the relative fine amount.

Authentication / ID Management. These activities are often weak and can be strengthened significantly. With respect to passwords (by far the most popular method of authentication / ID management) there are many shortcomings. Passwords can be hacked, cracked, or stolen allowing unauthorized access. The password field is the gateway for SQL Injection, the most prevalent form of attack as revealed in IBM's X-Force Report for 2009 with as many as 30 million attacks occurring per month. Many public and private sector websites and databases have been successfully breached by using SQL Injection attacks which are largely untraceable. Triad Biometrics' TEAMS® uniquely can defend against such attacks. Additionally, many

3701 FAU Boulevard, Suite 210, Boca Raton, FL 33431 USA • 151 June Road, Stamford, CT 06903 USA
561 394 7791 T 561 620 8493 F www.triadbiometrics.com 203 322 5100 T 203 322 9300 F

biometric systems allow multiple identities under the same biometric template or they permit multiple identities at time of enrollment. By utilizing 1 to many real time matching and alias resolution as well as robust encryption, many weaknesses could be removed in current systems.

Global Engagement. Global engagement should be coordinated by the United States as it developed the original framework for the internet without security and has an enormous amount of valuable data to protect worldwide. Incentives should be provided to members of a global forum to adopt standards established by steering groups within such forum. These incentives need not be monetary but could be a contribution of technology and expertise in hardening the infrastructure of participant countries.

An incentives framework for evolving cyber-risk options and cyber security best practices. This topic has been touched addressed from an international perspective. Domestically, there should be both positive and negative incentives for entities to follow best practices guidelines and to develop and implement technological advancements. Incentives could take the form of tax credits for R&D relating to improved cyber-risk abatement as well as direct government subsidies for such research. Additionally, entities experiencing breaches but employing the latest technologies could mitigate their exposure to fines or other negative incentives while entities not employing such technologies could face surcharges to fines imposed on them.