AMERICAN BANKER®
THE FINANCIAL SERVICES DAILY

Thursday, August 18, 2011

VIEWPOINT

Data Insecurity Is a Systemic Threat

EUGENE A. LUDWIG
PROMONTORY FINANCIAL GROUP

As if the financial system needed more challenges, there is a huge one that never goes away: keeping data secure. Because our current market and economic predicament has presented a barrage of other risks that are perceived as more immediate, securing customer and corporate data too often remains at the bottom of the triage list.

In the meantime, corporations continue to suffer major data breaches with discouraging regularity, and the risks are growing faster than our capacity to mitigate them.

The FBI rates cyberattacks as the third-greatest threat to U.S. security, behind nuclear warfare and weapons of mass destruction. Recent bank data breaches have been so severe as to merit mentioning in the first annual report from the Financial Stability Oversight Council. These attacks are "important reminders that both regulators and firms need to continuously upgrade the resilience of their electronic systems and networks," it says.

Finance is becoming ever more dependent on the Internet and all other manner of technology for selling products and completing transactions. In an era when clients demand more service and quicker speeds, retail banking continues to tilt increasingly toward branchless, paperless, electronic delivery systems.

Just consider paper checks, which are going the way of phones with dials and watches with winding stems — they are becoming a relic that folks will reminisce about over Thanksgiving dinner. Paper checks made up less than 25% of the noncash payments in the U.S. in 2009. Check use fell by $6 billion from 2006 to 2009, to $24.5 billion, while total noncash payments rose by 4.6% a year.

Breaches and hack attacks are common in business, and finance is particularly vulnerable to them.

This innovation has many benefits, but there are significant risks. Technology breaches, crashes and hack attacks are now common in business, and finance is particularly vulnerable. Finance is an information business, and information technology is at the heart of the technology revolution. As a result, banks are particularly susceptible to the costs of data security gaps and ruptures.

Every few days there are more revelations of data breaches, and it appears these problems are accelerating. The number of hacking incidents through July is outpacing last year, with a 370% hike in the number of records improperly disclosed than in all of 2010. That adds up to a flock of potential black swans.

The Internet was never created to be bulletproof from a data security perspective, and the current version is easily pierced. Cyberattacks are a distinct danger and not enough has been done yet to give confidence that protections will prove effective. Banks may enhance their own security, but remain highly reliant on third-party vendors, which may not be subject to the same stringent security requirements.

Recently , firms in the U.S. have been under "advanced persistent threats," which are conducted with intent by well-funded hackers. Vigilante groups or "hacktivists" have also targeted companies this year as a continuation of attacks in 2010 that were done to protest the suspension of services, such as donations and server hosting, to WikiLeaks and retribution to companies that have pursued hackers through legal and criminal proceedings.

Economic losses from hacking, including reputational losses, can be high for a company uniquely affected by a cyberattack. Aside from customers losses and replacement costs, there may also be market costs to victims of cyberattacks. Stock prices can be negatively affected to the tune of 1% to 5% in the days after a cyberattack, which

translates into losses of $50 million to $200 million for shareholders of the average NYSE company. Furthermore, being perceived as having less robust security than competitors can be detrimental to the bottom line. According to a Fundtech survey, 74% of bankers believe small and midsize business customers would switch to banks that offered better security.

As technology morphs further, cloud computing presents additional challenges. Data is coming off the hard drive and moving to shared data mechanisms provided by companies with better than average security, but offering bigger returns for successful hackers. Forrester Research projects that the global cloud computing market will grow from $41 billion in 2011 to $119 billion in 2014.

Of course, individual banks and associations are spending considerable sums to deal with this problem. However, more needs to be done. What should occur swiftly is for government and the financial sector to redouble collaborative efforts, setting high goals for minimizing data privacy and data disruption issues.

The recently updated FFIEC online banking authentication guidance endorses stress tests to highlight potential security breaches; it also endorses the use of layered security, including strong authentication, out-of-band technology and complex challenge questions. This guidance, in conjunction with customer education and vetting of vendors should, be implemented across businesses. Irrespective of whether such collaboration takes root, financial institutions and their boards of directors need to take these issues extremely seriously. Data security is an issue of potentially systemic proportion. ▪

Eugene A. Ludwig is a founder and the chief executive of Promontory Financial Group LLC. He was the comptroller of the currency in the Clinton administration.