Harrington, Chris

From: Haskins, Craig [chaskins@rsasecurity.com]
Sent: Friday, October 13, 2000 2:47 PM
To: 'chris.harrington@ots.treas.gov'
Subject: Comments on GLB, Title V, sec. 501

38

Chris,

Following are my comments on Gramm-Leach-Bliley, Title V, sec. 501. In short, sec. 501 addresses the need for financial institutions to provide security and confidentiality for customer records and information.

E-business has quickly become the norm, rather than the exception. The Internet has added to the complexity of corporate computer networks, blurring the distinction between outside the network and inside the network.
Unfortunately, the power of the Internet does not come without its risks.
Hackers now have an unlimited number of onramps onto the Information Superhighway making it easier to monitor, intercept or alter communications or transactions.

Even with the dramatic rise in security breaches, there is a significant lack of awareness as to how risky it is to rely solely on passwords for network access. While the financial risk is obvious, breaches also significantly damage a firm's reputation and could further serve to undermine the trust inherent in the U.S. banking system. Passwords alone cannot ensure secure access to e-business applications because they are a weak form of security that are easily guessed, stolen, or otherwise compromised. Once a password is compromised, a business entity has no idea whom they are doing e-business with. Two-factor authentication ensures greater network security than the traditional static password by requiring two forms of ID: something a user knows (secret PIN) and something a user has (a random, one time use authentication code). The typical user expects two-factor authentication when they use their ATM (their bank card and PIN).
Why shouldn't they expect the same when they are transacting over the Internet with higher stakes? Two-factor authentication should become the standard method of authenticating: remote employees accessing a corporate network, customers, partners, or suppliers accessing a corporate extranet or e-marketplace, or clients accessing a Web based application such as online banking or brokerage.

While a strong, 128 bit encryption standard can help protect the privacy and integrity of data traveling across corporate networks and the Internet, firms cannot feel totally safe in an e-Commerce environment without non-repudiation ---preventing a party from later denying that a transaction took place. Non-repudiation gives firms who are establishing an e-Commerce presence the assurance that the validity of a transaction, whether it is an online trade or money transfer, will stand up in court. The most efficient way for financial service firms to establish authenticity, privacy, integrity and non-repudiation of communications and transactions is by implementing a public key infrastructure (PKI). This is especially important now that the digital signature bill (officially known as the Electronic Signatures in Global and National Commerce Act) went into effect on October 1. This landmark legislation gives digitally signed on-line contracts the same legal enforceability as paper contracts. In this new landscape, a PKI can give firms the confidence they need to accept digitally signed documents, ensuring the authenticity of parties in an e-Commerce transaction.

Please let me know if you have any questions.

Craig L. Haskins
Financial Services Market Development Manager
RSA Security Inc.
"The Most Trusted Name in e-Security"
chaskins@rsasecurity.com
http://www.rsasecurity.com/ <http://www.rsasecurity.com/>
Office-973-597-0089
Mobile-973-568-4131