

Control Essentials

Volume II, Issue II

February 2007

Business Consulting

- *Regulatory Support*
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- *Enterprise Support*
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- *Application Security*
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- *Network Security*
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

Authentication in Banking

The FFIEC (Federal Financial Institutions Examination Council) guideline recommended the introduction of enhanced security authentication measures by the end of 2006 for all financial institutions offering Internet based financial services. They consider that a single-factor authentication is inadequate for high risk transactions involving access to customer information or the movement of funds to other parties. Although a number of the larger organizations have religiously adopted the FFIEC recommendations, a number of smaller banks have resisted.

Many smaller banks view the FFIEC recommendations more as “suggestions” rather than literal rules. While this is true to some extent, the benefits that banks can gain from adherence to the guidelines are significant. Banks will be audited against these recommendations provided by the new guidelines and once the deadline for compliance is reached, in 2007, federal examiners will document all cases where compliance is not demonstrated.

Why comply?

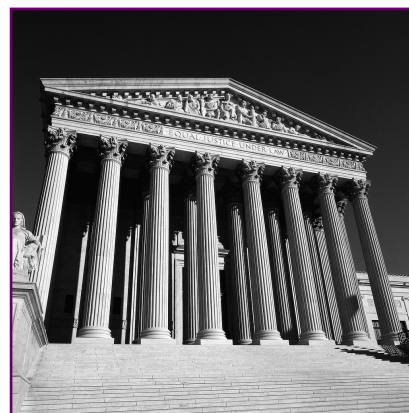
The continuous growth in cyber crimes such as phishing and spam has led to a heightened sense of apprehension towards online financial services, especially Internet Banking, within the user community.

Enhanced authentication mechanisms supported by specific measures to deal with cyber crime will help alleviate the fears of the customers. Studies indicate that an estimated 56 million households will bank online by 2008. The number could reach record heights if measures are taken to increase security.

Another big reason to comply is the increase in cyber attacks against small and mid-sized organizations. Many large organizations with a reasonable security budget have implemented stringent measures to counter cyber crime. A number of them such as the Bank of America and HSBC have already started to enhance authentication mechanisms. This has shifted the focus of the attacks onto the smaller organizations that are more vulnerable owing to smaller IT budgets and hence weaker security mechanisms.

What to do?

The first step to compliance is a Security Risk Analysis. A risk analysis aims to pinpoint specific areas of an organization's IT infrastructure that need immediate allocation of a share the security budget pie. At the end of a risk analysis, an organization can answer the all important question - “What are we protecting against?”



The next step is to conduct a Cost-Benefit Analysis to ascertain which type of authentication mechanism fits best into organizational budget and business requirements. There are two things that need to be kept in mind while choosing an authentication mechanism:

- **Value at Risk**

This is the maximum possible loss that could occur due to the risks that are identified. Quite logically, the cost of protecting an asset should be less than its value. An authentication mechanism that requires more funds to be deployed than the projected losses is hence not profitable.

- **Ease of use by the customers**

Another important consideration is whether users are willing to use the enhanced authentication means. A complex or time consuming solution is inconvenient and will often scare away the average user. Customer buy-in is imperative and requires steadfast efforts to generate awareness.

Methods of Authentication

So how does authentication really happen in the first place? The method by which users can be authenticated is by asking them to produce something that is unique to them. The existing authentication mechanisms involve three basic "factors":

- **Something the user knows**

Examples: passwords, PIN numbers, pass phrases etc.

- **Something the user has:**

Examples: token, smart card etc.

- **Something the user is:**

Examples: fingerprinting, face recognition, iris scanning etc.



The robustness of the authentication methods will depend upon the combination of the factors. Authentication methods that depends on more than one factor are more difficult to compromise than a single-factor method. Most of the account fraud and identity theft are the result of a single-factor authentication exploitation.

Some of the authentication methods that are enlisted in the FFIEC guidelines are Shared secrets, tokens, Biometrics, Scratch Cards, IP address location/Geo-location and mutual authentication.

Shared Secrets

Shared secrets are the oldest form of authentication. They include passwords, PIN numbers etc. Shared secrets can be used efficiently in mutual authentication as will be explained later.

Tokens and Scratch Cards

Tokens and scratch cards are something that a user has and this can be used along with a shared secret to implement two-factor authentication. However, the cost of implementation per customer can be prohibitive for smaller organizations. Customers might also not fancy the idea of carrying a device with them each time they need to use the service.

Biometrics

Biometrics uses methods like fingerprinting, face recognition and iris scanning. Each of these requires additional equipment to be installed at the user's end. With biometrics, however, the complexity of authentication could often deter individuals from using it even if the organization has the funds required to install scanning devices on user computers.

IP Address Location and Geo-location

The IP address location and geo-location involves determining the IP address of the system used by the customer and also the geographic location of the user. This is done by using sophisticated techniques that determine the time taken for internet communication to take place. This time is compared to distances of known locations. A reasonable match allows further communication. If not, the user will need to authenticate via telephone. But this technique is susceptible to IP address spoofing and also limited by its ability to determine distances only for wired clients.

Mutual Authentication with a Shared Secret

In this method, a user chooses an image and/or a pass phrase and checks for these at the time of each logon attempt. The user can now use the regular username-password scheme to authenticate with the website. This method relies only on shared secrets for mutual authentication between the website and the user, and therefore is not two-factor authentication. However, it adds an extra layer of security and can also bolster customer confidence.

Final Words – What's best for you?

The customer is all-important. Choosing the right authentication scheme requires an organization to assess risk in the light of the customer. Based on various focal points, such as customer type, nature of transactions, sensitivity of customer information, mode of communication etc., the overall risk involved is the first issue any organization should be concerned about. With an understanding of this risk, the choice of authentication infrastructure will bring with it both compliance and business.

The FFIEC guidelines suggest an improved authentication scheme supported by a strong security policy. With regulatory compliance being only a by-product, it is about time that smaller banks eye the profits that can be made by fortifying their defenses.



Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" accounting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

We encourage you to visit our website, www.emrisk.com, for details on ERM's services, team profile, clientele and testimonials from some of our clients.

For further information, please contact an ERM consultant at (305) 447-6750.