



Securing Internet Information Server™ (IIS) and Achieving Sarbanes-Oxley Compliance

Version 5.0: December 15, 2007

Case Study: United Security Bank (NASDAQ: UFBO)

Company profile

FOUNDED IN 1987, UNITED SECURITY BANK IS A STATE-CHARTERED INDEPENDENT COMMUNITY BANK HEADQUARTERED IN FRESNO, CALIFORNIA. AFTER FIFTEEN YEARS, THREE MERGERS AND FOUR BRANCH ACQUISITIONS, UNITED SECURITY BANK CURRENTLY OPERATES TEN BRANCHES IN FRESNO, MADERA, AND KERN COUNTIES, AND EMPLOYS OVER 100 PEOPLE. TODAY, WITH MORE THAN \$560 MILLION IN ASSETS, \$490 MILLION IN DEPOSITS AND \$380 MILLION IN LOANS, UNITED SECURITY BANK CONTINUES TO SEEK GROWTH IN ITS MARKET AREA WHILE ENHANCING THE FINANCIAL SERVICES OFFERED TO ITS CUSTOMERS.

Introduction

As has been the case for many years, Microsoft has been the underlying software of most computer systems. Whether it is a desktop, notebook computer or server, Microsoft software is present more often than not. With this large population of computer users, it has also been the case that computer criminals have focused on seeking ways to breach and steal information or conduct computer fraud on these computers. Hackers, viruses, malware and other Internet borne threats continue to plague personal computers around the world, either causing systems to malfunction, or resulting in the theft of information that can be used by the attacking criminal for profit. Notable breaches have occurred against companies that have government mandated regulatory requirements. These mandates include that proper IT procedures must be established that provide data protection to minimize and/or prevent computer crime.

Industry analysts continue to reinforce the need for behavioral software security to be a component of an organization's security strategy. Why? It can be said that all computer users are unique. No user operates a computer the same way as another. Whether they use a personal computer for e-mail, research, document preparation, data analysis, etc., a computer user will have different behavioral characteristics than another user. It is important for organization, as part of an overall information technology and security strategy, to consider computer system behavior. Behavioral anomalies are indicators that correlate to threats on computer networks. Implementing a technology solution into an overall IT strategy that can track and alert when system behavior should be questioned is a smart investment.

United Security Bank's Goals

As a local independent bank, United Security believes strongly in the principles of community banking - prompt response and superior personal service. USB staff has extensive expertise in such areas as commercial real estate and construction lending as well as small business financing that enables the bank to provide a quality level of service not found elsewhere.

The bank's primary business strategy is to focus on increased market share in the local community, as well as expansion into new markets when sound business opportunities present themselves. This growth strategy is based on enhancing shareholder value through increased and consistent net income and earnings per share. United Security Bank has consistently received the highest bank ratings for safety and soundness. The Bank consistently maintains a "Super Premier Performing Bank" rating as determined by the Findley Reports and is rated

outstanding by bank regulators in Community Reinvestment Act (CRA) performance. The Bank is also regularly awarded a “5-Star Rating” by Bauer Financial Reports, while Veribank recognizes United Security Bank as a top “Blue Ribbon Bank.”

Availing customers of transaction services through their full-featured online banking systems, is a major differentiator for USB. The bank remains very focused on adding safe and secure account management capabilities for clients to access via the Internet.

UNITED SECURITY BANK ...response ability

HOME RATES PRODUCTS SIGN-ON CONTACT US

	Last	Change	Percent
NYSE	10542.98	-1.92	-0.02%
NASDAQ	2145.91	-3.42	-0.16%
UBFO	28.14	0.00	0.00%

September 15, 2005

SYSTEM STATUS: UPDATE: United Security Bank now supports Quicken 2005 Premier Edition.

LOG ON

ABOUT US
INVESTORS
ONLINE BANKING
PRIVACY
USB E-PAY
GOVERNANCE
HOME MORTGAGES

CONTACT INFO
1.888.683.6030
info@unitedsecuritybank.com

Quick find

LOOK for a products or services

CHOOSE ONE

- Business Accounts
- Certificates of Deposit
- Interest Bearing Accounts
- Loan Services
- Other Bank Services
- Personal Checking
- Safe Deposit Boxes
- Savings
- BankNet

Stock or Fund Symbol

Basic Advanced

United Security Bank (NASDAQ: UFBO), selected a security solution for their Internet systems that would provide for a system behavioral baseline and be used to alert the IT security staff when system behavior was not within a pre-determined norm. Not just a typical system resources norm such as heavy CPU utilization, but when a non-typical user action had occurred. The bank selected ThreatSentry from Microsoft ISV Partner – Privacyware. The Web servers that have been secured are based on Microsoft’s IIS Web server software where the bank’s applications provided critical information processing on backend systems. Utilizing Privacyware’s behavioral layer technology, called the Adaptive Security Engine, the solution added a new layer of protection to the bank’s existing IT security strategy, which monitored and actively blocked any perceived malicious activity on their IIS servers. Additionally, the software easily integrated into their existing system event management solutions and also was easy to administer and tune through the Microsoft Management Console.

"Being a financial institution, Sarbanes Oxley (SOX) compliance has impacted our security efforts. Towards the end of the year in 2004 most of our efforts were directed at ensuring we were in compliance with this legislation and we are always working to make sure to maintain this level of compliance. ThreatSentry is an important part of that compliance since it is tightly integrated with our online banking product and was a notable enhancement to our security efforts."

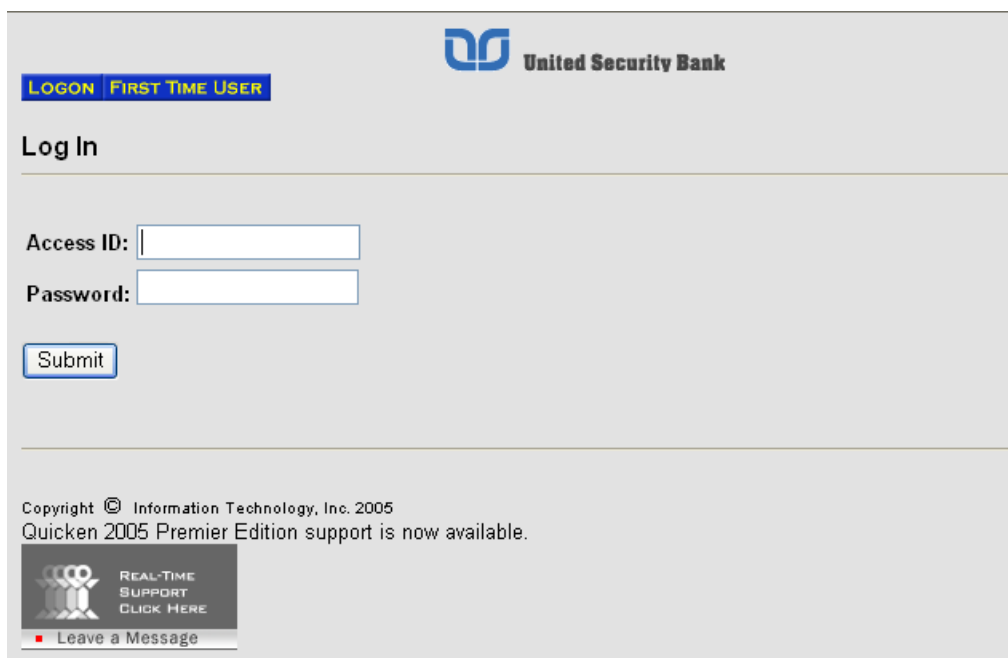
- Paul O'Neil at United Security Bank.

Reporting on the Web servers now includes critical security events, which provides a more complete and easily understood view into overall server session data. The software solution required a short period of time to implement and training included just two follow-up Web sessions, prior to ThreatSentry to be installed in production. What's more, at an investment price that is considerably less than any other IIS intrusion detection/intrusion prevention solution available, the software product continues to be an ideal, low-cost IT security augmentation that the bank was able to quickly implement without having to conduct an extensive ROI analysis prior to implementation.

Online Banking Specifications

The bank has taken further steps to prevent unauthorized use of their available, online services. Online banking can be used to access new or existing United Security Bank (USB) accounts. The services available to customers through USB's Online banking systems include:

- Obtain account balances on checking and savings accounts
- Check account transactions, such as automatic direct deposits and all branch banking activity, including up to date ATM transactions.
- Verify the amount of a direct deposit on its scheduled due date
- Find out what checks and withdrawals have cleared
- Transfer funds between USB accounts
- Obtain monthly statements on-line
- Generate reports on account activity
- Export account information and transactions to popular financial software packages
- USB will soon be adding electronic bill payment capabilities.



The screenshot shows the login interface for United Security Bank. At the top right is the bank's logo and name. Below it is a navigation bar with a blue button labeled "LOGON" and a link for "FIRST TIME USER". The main heading is "Log In". There are two input fields: "Access ID:" and "Password:". Below the password field is a "Submit" button. At the bottom, there is a copyright notice for Information Technology, Inc. 2005, a note about Quicken 2005 Premier Edition support, and a "REAL-TIME SUPPORT" button with a "CLICK HERE" link and a "Leave a Message" link.

Subscriber General Specifications

The following conditions must be fulfilled for the system to function properly and effectively:

The browser must preferably be Microsoft Internet Explorer 4.71 or higher, or alternatively Netscape Communicator 4.05 or higher.

For reasons of security and in order to provide better service to our clients, there is a 15-minute limit to complete transactions ("Process Timeout"). After the expiration of the 15 minutes the subscriber is automatically disconnected from the system. In addition, if after logging-in to the system the subscriber does not perform any transaction within 3 minutes, they are again automatically disconnected ("Idle Timeout").

Browser configurations are necessary to access the system online.

The secure mode must be activated (Secure Sockets Layer 2 and 3). Security selections are SSL3.0 and SSL2.

Javascript must be activated.

Style Sheets must be activated.

Security

United Security Bank has obtained the maximum possible security currently available on the Internet (128bit encryption). Thus, in every transaction performed, the messages exchanged between the client and the Bank's Web Server are encrypted. Currently, such encryption is available internationally in two levels:

40-bit encryption and 128-bit encryption.

The difference between them is considerable.

40-bit encryption means that there are 240 potential keys that may be used to encrypt messages, though only one functions on each on-line session.

128-bit encryption means that there are 2128 potential keys that may be used to encrypt messages, though only one functions on each on-line session. Therefore there are 288 times more key combinations than in 40-bit encryption.

USB provides the 128-bit encryption security level.

Beyond encryption, subscribers use personal ID numbers (User ID, Secret Passwords) to log-in, while the Bank also uses additional security systems (Firewall) which control and record each user's access to its systems.

Subscribers are responsible for safeguarding their personal security codes. In the event of disclosure to third parties, they must notify the Bank immediately.

Privacyware™ and Privatefirewall™ are trademarks of PWI, Inc. Products and trademarks from other companies mentioned herein are for identification purposes only and may be registered trademarks of their respective companies. Specification is subject to change without notice.

2005-2007© PWI, Inc. dba Privayware™. All rights reserved.