



Current Security Environment in the Financial Industry

Banks, credit unions and other financial institutions are increasingly sensitive to customer identity theft by hackers and sophisticated cybercrime attacks. In addition to electronically processing customer data, most institutions also support online banking and conduct e-commerce with customers and other enterprises. Security breaches such as identity theft and fraud have far-reaching impacts, ranging from remediation costs and damages payable to victims, to the cost of implementing new monitoring and intrusion prevention tools, to the inestimable toll of negative publicity and lost business.

Conservatively, the **Federal Bureau of Investigation** estimates that cybercrime incurs more than \$120 million in damages annually, and further that only 9% of cybercrime is even reported—which puts the cost of the total problem at a staggering \$1.33 billion annually. And the concern isn't confined to the FBI. A July 2007 report by the **Federal Trade Commission** confirms that email spam has become a significant global tool for the propagation of financial crimes, and the malicious acts of spammers and phishers are inherently criminal.

In response, a growing body of regulation imposes enormous burdens on institutions to exercise constant vigilance and implement safeguards to protect their information systems, transaction processes and customer databases. The Gramm-Leach-Bliley Act, Sarbanes-Oxley and others, enacted with the noblest intentions, present myriad requirements that can be challenging to itemize and understand—let alone implement and maintain. This Case Study examines how one Florida financial institution is addressing security compliance requirements.

BankUnited: A Solid Strategy

BankUnited Financial Corp. (NASDAQ: BKUNA) is the holding company for BankUnited FSB, the largest banking institution headquartered in Florida. BankUnited provides a full spectrum of consumer and commercial banking services, mortgage and loan products, and investment and financial planning services. The company's online banking products can be accessed through www.bankunited.com.

BankUnited competes with larger rivals through its neighborhood banking strategy, which targets consumers and businesses close to local branch offices. In addition, the company's ability to make decisions in the local markets enables customers to respond more quickly to opportunities. The benefits of decentralized decision-making and community engagement are promoted through the messaging, "It's a local thing."

"When it comes to managing customer data, retail and commercial clients have long trusted BankUnited for our security, speed, efficiency and value," said Adrian Diaz, assistant vice president of information security for BankUnited.

Objective Proof of Compliance

BankUnited was already observing recommended standards established by the Office of Thrift Supervision (OTS), and maintaining stringent security policies as well. However, compliance verification required an annual independent audit, so they turned to SECNAP® Network Security for assistance.

SECNAP was selected for the expertise of its security compliance auditors and comprehensive scope of its IT Security Audit services. The firm also follows a rigorous process to ensure every requirement is addressed. And as a trusted security advisor to many other financial institutions, SECNAP was well-positioned to assist BankUnited.

continued

Confirming Compliance through a Comprehensive Security Assessment

SECNAP Network Security performed an extensive external penetration test and internal vulnerability assessment utilizing its proprietary network scanning system to assemble facts about network strength, associated IPs, and the health of the Bank's security architecture. Central to the audit's effectiveness was the depth of experience and knowledge of the SECNAP audit staff.

"Our SECNAP auditor came to us well-prepared and highly experienced, which made the entire process extremely efficient," says Diaz. "He was technically adept and security savvy, and therefore was able to conduct a detailed, specific assessment of our network with virtually no learning curve."

BankUnited's network security standards and policies were well established, but the firm wasn't sure just how solid they were until the IT security audit was completed and a detailed assessment report presented. The report also recommended a remediation action plan.

"SECNAP identified a need for an internal logged wireless security detection process by playing a little hide and seek with us. In this case, it was 'hide-an-unconnected-wireless-access-point-and-see-if-you-can-find-it-with your-existing-tools.' This friendly but important test process brought to light the fact that we needed better tools than we were currently using," said Diaz. "We now have a process in place to regularly check for any wireless access points."

"SECNAP conducted a very thorough GBLA-focused audit and left no stone unturned. They even noticed physical security issues, such as when an employee had temporarily propped open a door to one of our computer equipment storage rooms."

— *Adrian Diaz, assistant vice president of information security, BankUnited*

Benefits Beyond Compliance

The scope and performance of the audit enabled the Bank to meet or exceed its internal security metrics as well as external regulatory requirements. Further strengthening its information security program also helped improve customer service and enhance its brand perception in the market.

According to Diaz, it is of vital importance that clients continue to have complete confidence that their bank is solidly meeting all compliance requirements.

Working with SECNAP to Strengthen Customer Loyalty

Exceptional expertise in network security and IT security compliance enabled SECNAP to deliver a highly efficient auditing and remediation solution that ensures BankUnited retains its respected position as a trusted service provider to its valued customers.

Clients are assured that BankUnited continues to meet the highest standards of data processing security and that their confidential information remains protected and secure. At the same time,

BankUnited has strengthened its brand as a solid, forward-looking provider in a highly competitive industry.

To learn more about SECNAP Network Security, contact your SECNAP representative at 866-732-6276 or visit www.secnap.com.

866-732-6276

