

Protecting Customer Data at Rest and in Motion

Banks have critical data residing not only in their core system, but throughout the bank on servers, desktops and laptops which makes protecting this diffused data very complex. The first step in ensuring that critical data is protected is to make sure the bank has completed a thorough hardware and software inventory. This inventory will be instrumental in determining where critical data resides thus leading to which systems need the most protection.

Encryption is a data protection alternative that is rapidly gaining popularity. Again it is critical to properly pick and choose which data deserves to be encrypted, and in what location. It is very important that the bank have written data encryption policies and procedures before implementing any encryption scheme. The encryption policy should clearly state the purpose of data encryption and what types of data, at a high level, are required to be encrypted. The encryption procedure should clearly state how the encryption will be accomplished and what specific data will be encrypted as well as where the encrypted data will be stored. In general, it is easier to encrypt data at rest than in motion, but both alternatives need to be explored. We like to use biometric technology with encryption/decryption because you always have your keys (your fingerprint for example) with you. Using a PIN code in conjunction with biometrics is acceptable as well. Multi-factor authentication is always better than single-factor authentication.

Banks should work with their outsourced vendors on their encryption policies and techniques so you can be assured that your designated critical data is being protected at all times whether the data resides on your own systems or is being stored at your vendor's facility. Banks should not just rely on audits, such as SAS70, with reports presented to them by their vendor. It is suggested that banks, whenever possible, visit the vendor's facility or hire their own consulting firm to review the vendor's facility and policies/procedures.

Traditional network security techniques still matter for banks such as vigilant system patching, up-to-date anti-virus/anti-Spam signatures to block Trojans and other malware, and properly configured firewalls especially with egress filtering enabled. So many organizations still protect networks from the outside in but neglect what may be allowed to leave their network. With malware rampant, if egress filtering is not implemented, your network could be used to compromise other organization's networks and could possibly subject your organization to liability. While it may seem improbable, phishing still remains a problem. Of course, identity theft is a very high priority with the Red Flags legislation and its accompanying policy, procedure and technology changes. Security awareness training is an area of concern - it must be ongoing and constantly fine-tuned to the bank's evolving policies and procedures. Finally, banks must ensure that they have a practical incident response plan in place, even if the chances of using the plan are very slim.

At Netsecuris, our staff has many years of experience working with financial institutions and other heavily regulated industries. We take our responsibilities very seriously and are very thorough and careful about the work that we perform for our clients. We pride ourselves on listening to our customers and helping them meet both their security and business goals. This entails taking the time to thoroughly explain their technology options and also researching the marketplace for the best - and most affordable - solutions that help banks stay secure. Because a bank's network infrastructure is so closely tied to information security, Netsecuris has staff dedicated to assisting clients with configuring and maintaining their networks. From infrastructure to managed security, Netsecuris assists banks with their information technology needs.



Leonard Jacobs
CEO

Leonard Jacobs is President and CEO of Netsecuris, Inc. Mr. Jacobs has many years of Information Technology and security experience working in the financial services industry, and holds numerous degrees and certification, including MBA, CISSP, MCP and CSSA. Netsecuris was founded in 2000 and is currently headquartered in the Minneapolis-St. Paul area. Their primary mission is to provide their customers with high quality and secure information technology solutions. They believe that business requirements should drive technology and they diligently follow this philosophy in all engagements with their customers.

