

## *Perimeter, Host and Endpoint Security – Finding the Right Mix*

Banks need to recognize that first and foremost, information security is a business problem not a technical problem. They need to understand their business goals and prioritize the protection of their customer information and computer and network systems based on those goals. Once they take a multi-faceted and in-depth look at their business operations, they can then put appropriate policies, procedures and technology in place to properly protect those assets.

The traditional network perimeter, 'protected' by just a firewall, is part of a wider realm that needs further protection today. Firewalls do not provide adequate protection because they are sieves today due to the need to open 'holes' in order for the business processes to function. Of course, banks must still defend the edge of their networks, but they are now tasked with looking for comprehensive ways to extend their protective measures throughout their entire network. For example, NAC (network access control) is one area that we see growing in importance. And of course, Network Intrusion Prevention Systems remain critically important to have in place and be properly configured. However, an area that is more lacking in attention to protecting network resources is host-based intrusion prevention as well as data extrusion prevention or sometimes called "data leak." Banks must take a multi-faceted approach to protecting their network infrastructure.

Information security management is a full time job and most banks simply do not have the resources to adequately manage the security of their network infrastructure. At Netsecuris, we offer banks the flexibility of either letting our highly experienced security experts completely administer the security of their network infrastructure, or we can establish a co-managed solution where we work closely as a team with their IT staff. Having worked as an information security manager, Mr. Jacobs understands how community banks operate with budgetary limitations, so Netsecuris is flexible in how solutions are tailored to each bank's specific requirements and budget.

Another big part of a bank's information security strategy is being able to successfully work with auditors and provide them with all of the information that they need at audit time. Netsecuris has a great deal of real world experience working with auditors and can offer specific and helpful advice to banks.

Netsecuris strives to be a 'one stop shop' by offering banks a wide range of services and products such as managed firewall service, managed intrusion prevention, managed email hosting services, vulnerability assessments, phishing and other social engineering simulations, risk assessments, secure network design and testing, and endpoint and desktop checks. Netsecuris utilizes different teams to handle the various services and products so that independence can be established and no conflicts of interest arise.

Netsecuris' business philosophy is closely aligned with banks' philosophy – provide the best quality, professional, and personalized service possible. Whether it is for information security/network products or managed security services, Netsecuris works hard to earn the trust of our bank clients everyday.



**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.

