

Perimeter, Host and Endpoint Security – Finding the Right Mix

In many respects, the network perimeter is effectively gone and has been for some time. That is because so many ports and services must be left open, both inbound and outbound, in order for the bank to conduct its business. When you add targeted phishing attacks, application layer vulnerabilities and the increasing complexity of the enterprise architecture, the number of fracture points in networks and systems is driving us to rebalance our security spending away from the perimeter and into the core of the infrastructure, all the way down to the host. Consequently, there is much more of a focus today on monitoring and protecting the inside of the network, particularly servers, workstations and laptops.

Because of the disappearing perimeter, I've long been a proponent of endpoint security, both for workstations and servers. By 'endpoint security' I mean intrusion prevention at the endpoint which goes far beyond the false sense of security provided by just anti-virus and anti-spyware solutions today. Endpoint security approaches the security from the inside out. This is a proactive approach to security in contrast with the reactive approach that inevitably costs an organization more money as well as adds incremental risk to their information, customers and even their business as a whole.

At ICS, we believe in a structured, methodical approach to risk management. After undertaking a comprehensive risk assessment, we recommend specific policies, procedures and remediation actions designed to deliver the most benefits at the lowest investment levels. We operate under the assumption that one or more layers will fail, and that other strong security measures must be in place to compensate. Because of the speed at which threats are created and evolve, banks must have adequate controls in place throughout their infrastructure to both anticipate the threats as well as eliminate them when and if they do occur.

A key part of protecting desktops and laptops is developing and enforcing a limited number of standardized configurations. We have developed a state-of-the-art system called SmartDesktop that accomplishes this goal quickly and easily. The solution streams the entire desktop – operating system and applications – to the user's computer every time they logon. The bank's IT Department focuses their attention on controlling patches, application updates and security settings from a centralized location which are consistently deployed across the bank. This kind of configuration and system change management solution yields significant returns and protection for our customers, while also allowing them to continue focusing on their business.

With over ten years of experience working with a wide range of clients from banks to educational institutions to governmental agencies, we know that creating a secure environment requires an ongoing commitment to proactively protecting critical data and systems as well as cultural change from both senior managers and employees. Much like the classic "Value at Risk" concept, - a confidence level metric applied to quantitative risk management for financial instruments and assets - ICS' approach is to help our clients align their security management program with their business risk management program. This methodical, objective approach to risk management takes much of "black art" out of information security, and helps our clients align their security management program with their business risk management program while also continually measuring the effectiveness of the program.



Stephen Goldsby
CEO

Stephen Goldsby is President and CEO of Integrated Computer Solutions, Inc. (ICS), an Information Security Consulting firm founded in 1997 and headquartered in Montgomery, AL. Steve has been an information technology and security professional since 1991. As CEO, he sets corporate vision and direction, establishes client relations, networks with other professionals, and keeps abreast of new developments in the technological field. Through hard work and dedication, ICS has grown from one employee in 1997 to nearly one-hundred employees today. As the executive responsible for launching and managing ICS, he has become a thought leader in the information security industry with broad technical and business expertise.

