Posted: 10/07/2006 | **By:** Bill Brenner

Banking on security checks and balances

John Petrie is executive director and CISO of Clarke American Corp., a San Antonio-based company that specializes in financial services-related products. For those who would target the company's computer assets, the attack vectors would appear plentiful.

There's a physical threat posed at the company's check-printing plants, where people often come and go around the clock. Plus volumes of sensitive customer information are stored on the network, including addresses along with phone, account and tax ID numbers.

With 4,000 desktops, 500 distributed servers and a sales force that uses wireless laptops, there are constant risks not only from bad guys to find and penetrate a weakness in the network from cyberspace, but also from a potentially malicious insider.

Despite these and other concerns, Petrie doesn't lose a moment's sleep. Would-be attackers have layers of virtual barbed wire to climb over before ever reaching the company's crown jewels. That's because Petrie and his team have invested plenty of time, money and effort on a security system of checks and balances, where the potential failure of one security device is mitigated by redundant defenses.

"We have a robust screening process," he said. "We have controls to double check who's accessing what."

The triple threat

Petrie divides his concerns into three so-called buckets: fraud, always a danger when check-writing products are sent through the mail to delivery locations; Internet security, specifically how to protect data integrity as information flows through the network; and physical security.

"A combination threat is what I worry about the most," Petrie said. "There's always the danger of being infected by a bot that's connected to a larger fraud ring or malware sent out by criminal and foreign organizations. The external threat to data posed by hackers who might gain unauthorized access is something we take very seriously."

If that weren't enough to keep the company's team of 150 IT staffers busy, there are also a variety of regulations to heed, such as the Gramm-Leach-Bliley Act and the Federal Financial Institutions Examination Council's (FFIEC) security guidelines. Clarke American's ownership recently switched from a British company to one in the U.S., which means it'll also be bound by the Sarbanes-Oxley Act come December.

Security strategies

His security program is based on ISO 17799, which is comprised of about 127 security measures organized into 10 sections that specify best practices for business continuity planning; system access control; system development and maintenance; physical and environmental security; compliance; personnel security; security organization; computer and operations management; asset classification and control; and security policies.

The purpose of the code is to be as comprehensive as possible, covering practices that are applicable to a broad range of endeavors.

"We use a layered security program," Petrie said. "User access is very restricted and is defined by what someone needs to get their job done and what their managers say they need access to."
The company also uses a network intrusion detection system (IDS), access control lists, firewalls, and all desktops are fitted with antivirus and antispyware software.

Clarke American also doesn't allow employees to browse whatever Web content they want. Petrie said there are strictly enforced limits to what users can access on the Internet. And while wireless devices are proliferating rapidly across the business world, the company's policy does not allow for widespread use of wireless technology. Petrie said that policy may someday change, but for now wireless usage is limited to the sales force, which uses wireless laptops.

"In some cases, our associates can use wireless if that's all that is available," he said. "But they must use a VPN."

Vendors of choice
As an example of the organization's security check and balances, Petrie pointed out that more than one antivirus tool is in use. "Our primary enterprise antivirus and spyware solution is McAfee, but we use several point solutions such as Trend Micro and Spybot, among others," he said.

For risk management, the company uses Herndon, VA.-based Cybertrust Inc. "They are our double-check," he said. "They scan our network, enterprise and perimeter to ensure all our systems are patched correctly and that all our antivirus signatures are up to date." Petrie also said the vendor reviews Clarke American's best practices to ensure they are up to date.

"In general," he said, "we use enterprise-wide solutions and several point solutions to add additional controls or mitigate specified risks across the enterprise. It's all about having a layered defense."

He credits that defense for the fact that in recent years the company has suffered no major security breaches, either from the inside or from hackers outside the network perimeter.