



# LBMC CLIENT SUCCESS STORY

“Tremendous customer service from LBMC...”

- *Andy Sisco*  
Associate VP for IT, AmSurg

## Quick reporting makes life harder for spyware

### Challenge: Spyware on the loose

Like many businesses, AmSurg Corporation has employees who use laptops on the road and then connect with the network when they return to the office. And like others, AmSurg has to contend with spyware that these laptops pick up elsewhere and bring back home.

Unchecked, spyware can slow down and render a computer virtually useless and can proliferate to other machines on the network. The IT department at AmSurg Corporation, a Nashville, Tennessee company that runs a national group of outpatient surgery centers, had been dealing with the problem reactively, repairing the machines when users complained about performance.

### Solution: Prompt identification and a custom report

AmSurg wasn't really looking to address the spyware issue when it installed an IDS, or Intrusion Detection Service, from LBMC Managed Security Services. The IDS device monitors traffic entering and leaving a company's network and is intended to identify viruses and other intruders trying to use the internet to infiltrate an organization's computers.

But spyware detection turned out to be a side benefit of the IDS installation, which took place in early 2009. The mission of spyware is to communicate back to an external host from its nest inside a company computer and it was during that communication process that the LBMC device was picking up evidence of spyware in AmSurg laptops and desktops.

Those detections enabled the IT Department at AmSurg to proactively go to those machines without having to wait for a user complaint, repair the damage, and prevent the spyware from spreading to other computers in the network.

At AmSurg's request, LBMC also designed a regular spyware report.

“What we've actually worked out is a report we get every week that has every workstation infected with spyware,” says Andy Sisco, Associate Vice President for IT at AmSurg. “LBMC worked with us to get an xml-formatted report that we can import straight into our help desk system. It creates a ticket for every computer that's infected.”

The report was created within a couple of days of the request, an example of what Sisco says is “tremendous” customer service from LBMC. Some IT vendors might take 30 to 90 days to start providing a similar report, he says, and others might not provide it at all.

“For most security type applications, custom reporting is either something you have to develop yourself or it's just not available,” Sisco says. *(continued on back)*



### The Client

AmSurg Corporation, based in Nashville, Tenn., operates a group of outpatient surgery centers around the country that provide a narrow range of high volume, lower-risk surgical procedures, generally in a single specialty.

### The Solution

Lattimore Black Morgan & Cain, PC (LBMC) has over 400 employees in three offices across Tennessee. The firm has a dedicated managed security services department that assists clients nationwide with keeping their computer networks safe. For more information, contact Thomas Lewis, (615) 309-2296, [tlewis@lbmc.com](mailto:tlewis@lbmc.com) or Marcie Angle, (615) 690-1993, [mangle@lbmc.com](mailto:mangle@lbmc.com).



Nashville  
(615) 377-4600

Knoxville  
(865) 691-9000

Chattanooga  
(423) 756-6585

## **Results: Speedier machines, better internal customer service**

AmSurg has seen increased productivity for computer users as a result of the spyware detection, Sisco says.

“If they get infected, they’re not having to wait until their computers become just unusable, he says. “We let them know that they have an issue and we fix it before it’s really a problem for them.”

That in turn has led to higher levels of internal customer satisfaction for the IT Department. Sisco says users perceive that “IT is proactively looking out for their interests as opposed to just being there to react when they have a problem.”