

# As threats grow, so do security firms

## MORE COMPANIES NEED PROTECTION AGAINST SOPHISTICATED ATTACKS

BY JEFF BOUNDS | STAFF WRITER

September 2008 was not an easy time to be in any business. It was an even tougher time to open a new office for a business, even in Dallas.

But that's what New York-based Stroz Friedberg LLC did. And since then, the cybersecurity and investigations firm has doubled its total headcount and is planning to expand its Dallas office.

A big reason for the growth: Attacks on corporate and government data and networks are becoming increasingly sophisticated and appear to be on the rise.



ERIN NEALY COX

"Even just (in 2011), there's been an uptick in hacker activity," said Erin Nealy Cox, a former prosecutor in the cybercrimes unit of the U.S. Attorney's Office in Dallas.

Nealy Cox, an executive managing director at Stroz Friedberg, also heads up the firm's cyber-response practice.

"It's no longer the case where the only companies that had to worry were banks and credit card processors," she said.

Now, everybody from pharmaceutical companies to retailers and firms in the energy space may be targets of groups ranging from criminals looking to sell stolen data to "hacktivists," or even state-sponsored cyberintruders engaging in economic espionage.

That, in turn, means business for firms that help protect data and networks or investigate cybercrimes.

Stroz Friedberg, for instance, hires former military and law enforcement officials to do everything from investigating and stopping data breaches to digital forensics and collection of electronic evidence.

"With these kinds of digital cyber-problems, you can't skimp on who you're going to hire to help you with them," Nealy Cox said. "These days, everything companies have are in their networks. The most critical asset you have is your data."

Particulars on Dallas' Stroz Friedberg expansion plans haven't been worked out yet. For now, 12 employees are in Dallas, and the company will be hiring certified forensic examiners, along with managers to oversee investigations. No salary ranges were available.

Numbers are hard to come by on how many corporate data breaches occur in the Dallas-Fort Worth area or nationwide, largely because most companies try to keep them quiet for fear of litigation, embarrassment and the possibility of becoming a target again, experts said.

In a similar vein, nobody really knows the monetary damages U.S. businesses suffer from computer-based intrusions, often because the companies themselves don't know what data were compromised.



JANE DEAN

**GUARDING AGAINST BREACHES:** Credant Technologies, founded by Bob Heard, plans to expand its security offerings into cloud computing — a buzzword for outsourcing software, data centers and other headaches — and to boost its headcount 10 percent to 20 percent over the next year.

But recent high-profile incidents show why executives responsible for data and network security have reason to lose sleep:

■ On Christmas Eve, a group of hackers known as "Anonymous" swiped credit card and other data from Stratfor Global Intelligence, an Austin security concern. That same Anonymous collective in September attacked computer systems of various Texas police agencies, ostensibly to shine a light on corruption, published accounts say.

■ News surfaced in December that China-based hackers had infiltrated the computing systems of the U.S. Chamber of Commerce, including data on its 3 million members. The *Wall Street Journal* reported that the electronic break-in, which was shut down in May 2010, may have given the intruders access to the chamber's internal network for a year before it was detected.

■ In a November report, U.S. intelligence agencies accused the Chinese and Russian governments of pilfering American technology, with Chinese agents being "the world's most active and persistent perpetrators of economic espionage." Even some U.S. allies and partners "use their broad access to U.S. institutions to acquire sensitive U.S. economic and technology information," according to the report from the Office of the National Counterintelligence Executive.

Complicating matters is the plethora of electronics that expose data and networks to the bad guys. Whereas compa-

nies once stored most of their information on mainframe computers, data now can be found in places like embedded devices and industrial control systems, according to Toralv Dirro, a Germany-based security strategist at McAfee, a cybersecurity concern that is a unit of the California chipmaker Intel Corp. "There are so many more fields to secure," he said.

At the same time, vulnerabilities in corporate networks present opportunities not only for mischief makers, but for entrepreneurs as well.

A decade ago, Bob Heard founded Credant Technologies Inc. to help secure any computing electronic device that is connected to a corporate network, be that a wireless phone, a home desktop personal computer, a tablet or any other number of gadgets.

Today, the Addison business has 120 employees and plans to boost its headcount 10 percent to 20 percent over the next year.

Credant has plans to expand its security offerings into cloud computing, a buzzword for outsourcing software, data centers and other headaches to an outside party. Employees are increasingly bringing electronic devices connected to cloud services into their workplaces. That improves productivity but also has a dangerous side, Heard said.

"That data is stored in cloud services with minimal security around it," he said. "That's a catastrophe waiting for a time and a place to happen."

## No incentive to invest in cybersecurity

For vendors of products and services for protecting data and networks, there is sometimes an uphill climb to get corporate clients on board. Firewalls may provide protection, but they don't generate revenue.

"There's no economic benefit to invest in cybersecurity," said Jon Shapiro, director of cybersecurity business development at the University of Texas at Dallas. "There's no incentive to tell anyone when you've been hacked. There are no repercussions for not telling anyone."

That could change soon, at least for companies that have reporting obligations with the Securities and Exchange Commission. The Corporate Finance Division of the SEC issued guidance in October that said reporting companies "should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."

That guidance is advisory in nature and does not create or change SEC requirements, according to published accounts. But in a November op-ed piece in *The Washington Post*, two influential voices — Sen. Jay Rockefeller, D-W.Va., and Michael Chertoff, former secretary of homeland security — said the SEC guidance "is critical because it allows market participants to weigh cybersecurity as an investment factor."

jbounds@bizjournals.com | 214-706-7122