BUFFALO
BUSINESS FIRST

JUNE 1, 2017

CYBER SECURITY

Hackers, Beware of Shatter I.T.

BY DAN MINER
dminer@bizjournals.com
716-541-1616, @BfloBiz_Miner

Shatter I.T. has long been known as a provider of high-level technology services to clients, with a data center in Buffalo and round-the-clock monitoring from its network operations center.

It's been a good business for the company, which was founded by chief technology officer Mark Musone and added two co-owners in 2007: President and CEO Peter Ronca and chief operations officer Suzanne Furlani.

But the future is in security.

While a wave of ransomware attacks over the past few months awakened the public to a new era of internet hacking, Shatter has been working for more than a year to become an expert in cybersecurity.

The company's NOC has been upgraded to a security operations center (SOC), which means that its software, employees and technology are attuned to the probes of digital pirates and can stop attacks before they do any damage, whether they occur at 2 p.m. or 2 a.m.

The shift is driven by a fast-changing marketplace that includes dire threats to any business hosting data on the Web and a U.S. regulatory environment that demands anybody dealing with medical or financial data have secure systems.

"If you're a small company and something bad happens, you rarely ever recover," Musone said. "So people are taking it seriously. The government is enforcing regulations. And Shatter is in a unique position in that we can proactively monitor the security of your systems."

Shatter is not abandoning managed IT services, but Ronca said security is what's expected to drive growth in the next few years.

He projected that the company's head count will double this year alone and hopefully will push to 30 employees by the end of 2018.

Musone is a recognized expert in cybersecurity, having done oversight and audits for government agencies for more than a decade.

He said the SOC will look at a company's entire system of data, giving it visibility that's a necessary part of protection.

JIM COURTNEY

Mark Muscone, chief technology officer at Shatter I.T., says new cybersecurity services will be popular well beyond Western New York. He founded the Buffalo company as a managed services provider and data center.

For instance, Shatter will be able to determine whether a user is repeatedly typing a password entry because they can't remember it or whether a hacker cartel is probing the system looking for weaknesses.

"In the past, you had time to react to a hack and deal with it," Musone said. "But you're not dealing with kids anymore.

"These are international cartels that can take hold of your data and hold it hostage in an instant."

Health care is expected to be an especially large market for security services, as the federal government started actively enforcing HIPAA privacy laws and doling out significant fines to any health care entity that doesn't properly protect its data, Musone said.

Thus, Shatter executives said they offer an attractive service to something such as a health sciences startup or a doctor's office, which otherwise would have to establish their own cybersecurity operations.

The same dynamic is true for other industries that collect private data, he said.

Shatter's clientele has mostly been regional over the years, and Upstate New York will again be a focus for the security services.

But it is a national marketplace, and Ronca said the company's relatively low costs from being in Buffalo will end up attracting clients from places such as New York City.

Shatter is doing internal and external beta tests on its security, training its own employees on the new system.

The company expects to fully launch its security services this year.

Ronca said he's excited about a new phase of growth and is bringing on talented professionals who have the opportunity for advancement as the company expands.

Shatter is comfortable in its location at the Main Place Tower , which hosts the data center, security operations center and administrative offices.

But if the envisioned trajectory comes to fruition, additional office space may be required.

"This is going to be a much more effective option than trying to build a cybersecurity operation yourself," Ronca said.

"You'd have to hire the right people, implement it and then keep up with what's happening on a regular basis. That's all we're going to be doing."