Are You Protected Against Cybersecurity Threats in Your Business?

CONTRIBUTED BY DIAMOND TECHNOLOGIES, INC.

For nearly 25 years, Diamond Technologies has been on the cutting edge of systems and integration technology.

Diamond Technologies was a software development company that has successfully evolved into a systems integration, support, and consulting organization for public and private partners. With 50 employees, the firm oversees system management across numerous states. Locally, solutions span across several Delaware agencies, along with notable private clients including, the YMCA, Bank of America, Henrietta Johnson Medical Center and BrightFields environmental services.

But the more technology businesses use, the more access points for cybersecurity attacks there are, and some attacks are already on your computer right now. Diamond Technologies Vice President of Security and Architecture Duncan Bachen said that in recent years, it has become exceedingly difficult to secure corporate infrastructure with technologies from the past.

Even with the best virus protection out there, Diamond Technologies estimates that more than 99% of all attacks in the past year relied on human error to allow a security breach. Sixty percent of small to midsize businesses within six months of a cyber-attack go out of business.

Bachen's vantage point, most businesses are aware of security issues like phishing or clicking on an ad that contains embedded viruses. But what he is seeing more of these days is hybrid attacks where viruses are piggybacking on authentic software that is downloaded online.

Often, those viruses, attack vectors and automated scripts are looking for one thing: complete access.

"The people who send those out don't care about the administrative assistant or the engineer. They want the person who has all the keys to all the doors inside," he said. "And once they get in, they get everything. The theory is to attack the one person who is credentialed."

To head off internal attacks, Diamond Technologies recommends implementing Zero Trust framework, or an attitude of trusting nothing, verify everything and limiting access inside the company. The strategy aims to reduce the bad actor's chances to get access into the system.

"It may seem like it's overkill, but it's set up so that no specific user has any real privilege, and they are limited to what they can do," Bachen said.

"Most business owners understand the risk, but then they get a little leery about slowing staff down," Bachen said. "The compromise needs to be how to put the security in such a way to keep them doing their jobs."

What sets Diamond Technologies apart from other firms in the region is that its team includes those with backgrounds in major manufacturers, banking, pharmaceutical companies.

"With the team we have hired, we've created a warehouse of information to better protect companies, so companies don't have to build the system on their own."

Duncan Bachen is vice president of architecture and security services at Diamond Technologies. He has been an IT professional for over 25 years, and is certified as MCSE, MCSA, and MCP, pursuing a CISSP and CEH. Visit diamondtechnologies.com to learn more on securing your business.