CLINE WILLIAMS

EMPLOYEES AND TECHNOLOGY: DO YOU HAVE A HANDLE ON SECURITY?

A recent security incident at a water plant in Oldsmar, Florida demonstrates the risks of letting employees without training in security set up a computer environment.

News reports indicate that hackers gained control of an industrial control system responsible for water treatment - and instructed the machines to inject chemicals into the water in quantities thousands of times higher than would be safe. Fortunately, the water plant regained control of its systems before the water was poisoned. A review of how it happened, however, suggests that non-technical employees with the best of intentions may have set the stage for an easy hack.

Tech articles about the hack say that the water plant was running outdated software on an outdated operating system, which always increases the chances of an intrusion. In addition, the water plant employees all shared one set of credentials to log into the system remotely - a huge security no-no. Finally, the control computer was connected to the internet directly, with no firewall or other access control technology, exposing the vital system to literally the entire world of cybercrime. The town appears to have done virtually everything wrong.

Employers should draw a lesson from this incident. It's easy to say that only professionals should assign technology tools to workers, and that the deployed environment should be non-negotiable. Certainly, infosec pros should be keeping track of the latest updates for the technology your business uses. At a minimum, you need to make sure patches and security updates are timely installed. But locking your rank-and-file employees out of the discussion about the tools they need ignores reality: Your best workers will want to find efficiencies - to do more with less, and to use technology to improve their work lives.

Rick Jeffries, who leads Cline Williams's technology practice, recommends the following:

1. The deployed environment should be installed and maintained by professionals trained in information security. Employees generally should not have the ability to download software on their own.

2. That said, employees should have a voice in what tools they use to work. "Power Users," the class of tech-savvy employees who know enough to be dangerous, should be recruited to suggest and test new software and technology that can help your business realize new efficiencies.

3. Don't overlook your less-sophisticated employees. They can help you identify the repetitive drudgery, or the tasks that require too many steps to complete, which are also opportunities for automation and invention.

4. As always, train your people! They need to understand *why* it's dangerous to concoct home-brew solutions to business-grade problems. But use it as an opportunity to engage – give your people a voice in their productivity, and you'll receive dividends in security and efficiency.

To listen to a recent podcast featuring attorneys Rick Jeffries and Tara Stingley discussing these issues, please CLICK HERE.

To learn more information on these issues, please reach out to Rick Jeffries or another member of Cline Williams' Labor and Employment Law Section.