LARGE OR SMALL, LAW FIRMS ARE LEARNING THEY MUST DEAL WITH CYBERSECURITY

By Julie Sobowale

It's another busy day at the office when you receive an email with an attached memo. You don't remember asking for the memo, but you download the attachment anyway. Alarm bells! It's not an attachment. It's malware that's now infecting your computer and every other computer in your law firm.

This was the situation that Jessica Mazzeo and Fran Griesing faced. In July 2016, the computer system for their small Philadelphia firm of 12 lawyers was infected with malware. They contacted Integrated Micro Systems, their outsourced information technology provider.

"We caught it almost immediately," says Mazzeo, chief operating officer at Griesing Law. "We took down our network and ran virus software on every computer in the firm. Once we located where the virus originated, we wiped the hard drive."

That incident changed the way the law firm dealt with websites, emails and mobile devices. As a small firm, Griesing Law leans on outside providers for help. The firm uses Workshare, a cloud-based program that allows users to send files securely online, and Trend Micro to quarantine suspicious emails. It also made firewall changes to block certain websites from being accessed by employees because of the risk of malware. A new policy was implemented last year on internal email: If the source is unknown or if you're not expecting the email, don't open it.

PHOTO ILLUSTRATION BY BRENAN SHARP

MANAGING CYBER RISK