How to Protect Your Law Firm From Ransomware

By Tracy Schorn

May 23, 2017

Ransomware, a criminal enterprise in which malware encrypts data and keeps it hostage until the victim pays a ransom, is a billion-dollar-a-year business, according to the FBI. WannaCry, the most recent global ransomware attack, infected over 200,000 computers in 150 countries, primarily immobilizing health care centers.

Sharon Nelson and John Simek of Sensei Enterprises, Inc. warned that law firms also are a target for such attacks because of their sensitive data. Speaking at the third Practice 360º | A Day for Lawyers & Law Firms on May 19, Nelson and Simek said data breaches are particularly troublesome for the legal profession due to the ethical obligations of lawyers to keep their clients' information confidential and safe.

"You don't have to be a big firm to get [attacked by] ransomware," said Nelson. Smaller and solo firms are often more vulnerable because they don't have the same IT resources as larger firms.

The impact of ransomware goes beyond the loss of data and money. After a hack, 15 percent of data is unrecoverable and 85 percent is infected, businesses go offline for at least a week, and, worst of all, client trust is lost, said Simek.

Two-thirds of all malware comes via email attachment, and one in 14 people will fall for phishing emails, Simek added. So it's essential, he said, to create a workplace culture that practices cybersecurity.

Users click on phishing emails out of curiosity (racy photos), fear (a "bar complaint"), urgency, and recognition ("you've won an award"). But studies have shown that just one phishing simulation with employees can reduce the risk by 20 percent. One trusted source for simulation emails is Open DNS.

Another way of identifying email scams is to look carefully at the return email address and see if numbers have been swapped out for letters (i.e., smith@ao1.com instead of AOL), said Nelson.

Nelson also advised lawyers to check their insurance policies. "If you are hacked, know what your insurance company will do," said Nelson. Often policies will only cover physical damage, not data damage. If you want data damage covered, Nelson said, "get it in writing."

Simek and Nelson identified the following best practices for a cybersecure workplace:

- Disable macros
- Apply patches and software updates
- Run in least privilege mode
- Train end users about malware
- Encourage users to report infections
- Have an approved device policy
- Back up all data to both the cloud and external drives (and unplug after backing up)
- Test backups

If you find yourself infected, restoring your computer is not a job for amateurs. "Call a pro. It's just too important," Nelson said.