Investment Company Institute

Global Cybersecurity Forum

What to Know About Ransomware

Tony Cole, Vice President and Global Government CTO, FireEye: It's a scary, new trend, and we saw a significant uptick last year. In our m-trends 2016 report, which looks across 2015, we see more and more financial services, or FIN, attackers actually going through and attacking hospitals, healthcare organizations, banks, and other organizations where they can encrypt the data and then hold it for ransom. So they either encrypt the data and hold it for ransom, or release some of the data to prove they had access to the systems. Quite often we've found that sometimes they don't even really have access to the systems. They've just found some open dataset, published it, and then pretended they had access to a system. So they're holding somebody's data for ransom that they don't actually have access to via the system. A major concern is that these types of attacks are going to increase in complexity and hit even more organizations in the future.

Stephanie Ortbals-Tibbs, Director, ICI Media Relations: What should people in a business like ours do? How should they brace themselves for this trend?

Cole: I think one of the things you definitely have to do is work harder on understanding attribution. Who are the potential people who want to attack you and what are you doing to ensure that you're safeguarded? You should know your assets and safeguard them by making sure you have updated operating systems, which means you have the latest versions of them and that they're patched. Then you should actually look at threat intelligence as well, as a component of understanding who is going to attack you and ensuring that you're prepared.