A stormy road to cloud security

Although only a handful of people in the 500-plus person opening main session for SecTor 2009 raised their hands when asked if they had responsibility for securing their employers' cloud efforts, presenter Christopher Hoff had a bold prediction for the rest of his audience.

"The rest of you, by this time next year, will all be doing so," he said.

Hoff, a 15-year veteran of the security business and blogger focused on virtualization and cloud computing security, opened the show at the Metro Toronto Convention Centre with an overview of the challenges around securing the broad and all-encompassing cloud.

The biggest challenge, Hoff said, was the fact that the cloud was, by its nature, Internet-based, and "the Internet is a remarkably frail operating system," based on loose handshakes and trust. Hoff said that the technology industry is "product rich and solution poor" when it comes to security

"Our answer has always been the firewall and SSL, and that's simply not going to work," Hoff said. "The security industry is hard-coded on the wrong set of capabilities at the wrong time."

The move to hosted software (Software as a Service) hosted infrastructure (infrastructure as a Service) and hosted platforms (platform as a service) will mean IT has to address a variety of models, each with their own challenges. While SaaS offers a fair bit of security because it's a single, locked down application, it offers lesser ability to integrate with other products. Platform as a service is more extensible because it's based on APIs that allow access, but ultimately less secure out of the box, and IaaS swings the other way from SaaS, offering a great deal of flexibility and extensibility, but a much murkier path to manageable security.

The cloud will not, Hoff suggested, prove a cure-all for ailing IT practices found in the old world. In fact, it may exacerbate them.

"If your app development process sucks prior to cloud, it's going to suck as much or even more after moving to cloud," he said.

Hoff advised close attention to the details of the service level agreements that govern cloud relationships, and noted that many of the major public cloud providers include legal terminology along the lines of "you bear sole responsibility" and "you are responsible for your own password and any use of it." About the best case of SLA security language Hoff cited was that of Salesforce.com, which offered vague promises that "we shall maintain appropriate safeguards" for data.

He said that SaaS vendors are going to have to get more realistic with their terms, and often get caught up in the idea that because IT has failures, they should be allowed downtime as well. But SaaS providers typically only have to lock down one application in one browser-based environment, as opposed to the multitude of apps and environments run by a corporate IT staff.

Ultimately, Hoff said, companies have to be able to trust their cloud computing partners, but shouldn't trust too deeply. He cautioned that those who single-source their infrastructure to a single provider are creating a single point of failure, and are likely to be unpleasantly surprised by the way things turn out.

Help is on the way, though Hoff asserts "bad things are going to happen" in the cloud security space, he said

that “a lot of smart people are starting to work on these projects. In the end, finding hybrid approaches to handling security between the virtual and the physical will be key, as will visibility and service transparency.

“Given the short time framework of the development of the cloud, a lto of people who weren’t think of security before are doing so today,” he said.