Ryan Somma

Collaboration Tools and Information Security

The prevalence of collaboration tools will mostly negatively impact Information Security. As we learned in Chapter 4, people are the first line of defense in enforcing a secure environment, and collaboration tools like instant messaging, wikis, and e-mail provide additional mediums for security breaches.

Unless located on a secure intranet, a team working on a wiki for business collaboration is exposing their work to the world. Instant messages and e-mails sent out of a secure system are no longer secure. Most WAN business operations must go from one intranet to another, traversing the extranet.

Then there are the people themselves. A user who works on a intranet system during the day, and then uses a RAZ token to remote desktop into the system at night is fairly secure, but not if they e-mail their login details from their business e-mail to their home yahoo account for convenience. Similarly, if the Information Security Team chooses an insecure Instant Messaging system, one that does not allow limiting messages to and from a select group of people, or if a user installs one themselves without approval, then that software is broadcasting the IP address to the extranet and has opened a connect through security for others to exploit.

Speaking to virtual communities specifically, if, say, a business were to limit all interactions between employees to Second Life, completely prohibiting collaboration through other mediums, then security would improve, but at the cost of productivity. Second Life and other communities allow for total control over who is allowed into the system and complete transparency of transactions for management to observe. Such a

system, however, would currently be impractical. Personnel who are required to put all e-mails, power-point presentation, videos, and teleconferences through Second Life must also deal with the technical complexities of porting all these technologies to this medium. It takes significantly longer to have a meeting in Second Life than it does to just pick up the phone and dial into a teleconference.

There are strategies for using collaborative tools to improve information security. Collaboration tools are all about spreading information through the organization; therefore, a wise Information Security team would do well to use them for educating personnel on best practices and threats. E-mails from the team could warn personnel about new phishing scams, malware threats, and phone scams. This way, collaboration tools become a means of "circling the wagons," when an external threat manifests.