

Mind Your “P’s” and “Cues” When Securing Your Converged Network

By Darrell Epps, Forsythe

Volumes have been written about securing converged networks. There is a dizzying array of “reference security architectures,” “best practice solutions” and “industry leading products” out there in the market. At times it feels like the choices are overwhelming and the challenge of operating and maintaining a secure converged network in the face of all of the existing and emerging threats is virtually impossible.

So how do you filter through all the information and recommendations to determine what makes the most sense for your network environment? If these choices and the associated challenges seem overwhelming to you as well, my rule of thumb is to “mind your P’s and Cues”.

POLICY

Policy is (or at least should be) the foundation for everything else. It is the cornerstone for those attempting to operate a properly secured converged network as well as those contemplating migration to such an environment. Unless they are implemented and operated in accordance with a comprehensive, well-written, regularly maintained and updated, vigorously enforced security policy, all of the best security products, tools, and solutions available on the market today mean nothing.

Because network failures and outages in a converged network have the potential to cripple voice and data communications at the same time, it is imperative that your security policy address this risk with sound disaster recovery guidelines. Likewise, the security policy should address all known or anticipated threats, and lay out guidelines for addressing all known vulnerabilities.

Examples of some of the more common topics a security policy should address (by no means an exhaustive list) include:

- Operating system and application software patching policies
- Anti-virus software use and update policies
- Acceptable network use and access policies

- Password use and maintenance policies
- Physical access policies

Much has been written about what a security policy should contain, and many organizations engage outside consultants to help them with this step. The key is to make certain that 1) you have a policy and 2) you treat it as a living document to be updated as the needs of your business change and the inherent threats and vulnerabilities change and evolve. A static policy is worthless in the face of a changing business environment and changing threats and vulnerabilities.

PRUDENCE

Once you have the security policy in place, you must exercise prudence (sound business judgment) in deploying or managing and operating your converged network environment. Most businesses don’t operate very well or for very long without reliable dial tone or when their key applications are down. Because voice and data services run on the same network infrastructure in a converged environment, the business impact of outages is potentially huge and can result in devastating loss of business and/or severe damage to your company’s reputation.

Thus, if you are planning to migrate to a converged environment, prudence dictates not only a network vulnerability assessment prior to migration, to identify existing threats and vulnerabilities so these can be addressed, but a post-implementation assessment as well, to identify any unanticipated vulnerabilities or newly introduced threats.

If you are already operating a converged environment, prudence dictates performing a vulnerability assessment on a regular basis so that your network can continue to adapt and respond to the rapidly changing threat and vulnerability landscape. Similarly, if business changes and demands dictate significant changes to your converged network environment, it would be prudent to re-assess network vulnerability to ensure that any new risk is suitably addressed.

PERSISTENCE

You must be persistent in enforcing your security

policy rigorously and in keeping it up to date. And you must be persistent in testing your converged network environment to ensure that you know of and have a plan to address all current threats and vulnerabilities. Threats and vulnerabilities evolve and business priorities change over time. So must your security policy! This is the only way for all the effort spent creating the policy to pay off and of course the only way to truly mitigate risk.

Don't Forget the "Cues"

Watch for cues that it may be time to review and update the security policy or perform another vulnerability assessment. These cues include news coverage of a new worm, virus or other threat, major changes in business plans or business direction, or large scale changes to the converged network environment.

Prudence dictates that persistence in maintaining and enforcing your security policy is the correct course of action. Keeping current requires watching for the cues that it is time to review or re-assess that policy. By minding the "P's" and "Cues", you maximize the probability that your converged network will behave appropriately in support of your business needs and objectives.

Darrell L. Epps, Director, Network Solutions for Forsythe Solutions Group, has more than 20 of experience in networking and IT and numerous manufacturer certifications. His broad experience, which includes network and IP infrastructure project management, implementation engineering and operations support, has provided him with a thorough understanding of project lifecycle issues at every phase of execution.

