Network Threats and Risks

By Hunter Newby

Focusing too much attention on the applications that ride over IP on the public Internet is perilous. Blindly believing that all of those applications are "safe" and "secure" is just as ignorant and this is not limited to the application itself being hacked or breached in some other way. The entire process of application delivery is at risk.

Application delivery is basically the initiation of the "session" (whatever that may be) and the continuation of it until the user completes the session or transaction and it is terminated. Anything that blocks, materially slows down or prematurely terminates the session is a threat. Some examples of sessions are VoIP, web browsing and ecommerce transactions – almost anything on the Web part of the Internet.

The threats range from intentional, malicious attacks such as spam jamming, packet blizzards, DoS in the higher layers, physical cable cuts at various network points in the lower layers to the natural evolution of clogged network arteries through overselling and under-provisioning. The malicious acts in the higher layers can cause congestion from the standpoint of rendering routers unable to process. That can be overcome and routed around, but it is still an issue, albeit temporary.

The higher layer risks also are usually perceived by the layman as something that the "techie" people are addressing and must fix. This is a major issue in and of itself as no issue should be minimized and dismissed as "not my job", but considering that it takes a certain level of technical comprehension to understand and properly address the problem, the incapable are probably doing the capable a favor by getting out of the way.

Challenges with the next level down from the software and application layer – the illusive Internet service provider capacity issue – are easier to comprehend, but still obscure. You may be content with your provider's throughput and latency. If you are really good, you manage your own routes, but there are many buyers who don't. They just rely on the ISP and say, "Hey, they are the professionals and this is their business." That mindset doesn't help much when the ISP is having an outage and has no answers.

The real underlying issue behind the ISP (Internet) backbone capacity risk is whether or not the provider has the network in place today and the cash to afford the necessary upgrades to support the amount of capacity it has sold and committed to providing to its customer base. This is a difficult situation to address. What ISP really knows what their network exposure is every day down to the megabit level on each link and is prepared to absorb spikes without affecting QoS? There are probably a few and they can afford to build out the required access and core connections to keep the machine moving smoothly. The rest are playing a ratio game whose numbers were created in the 1990s based on old school web traffic. There are no historical models for web video traffic and the impact that has on the aging access and core links of yesterday's ISPs. How does a buyer even ask an ISP how well they are doing in this regard? How would an ISP respond? Is it even possible to give a response that is remotely honest and accurate?

In this scenario service providers don't know the answer. As congestion spots arise they are addressed like brushfires springing up here and there. They hope that the fires don't catch a good wind and spread to the rest of the network. Most of them hope that the heartburn will just pass on its own. One day if they keep going this way the elephant is going to sit down on them all and network cardiac arrest will ensue. Proactively dealing with this requires acknowledging that the risk exists and regularly visiting the network doctor to check on the arteries.

It is in the lower layer where the risks are much easier to understand and deal with that the invisible protective barrier of ignorance doesn't really exist and should not be allowed. Physical layer weaknesses can be found by simply looking at a fiber or other physical media network map. Any place where there is a linear path with insufficient or no redundancy is a fault line. The only complexity in dealing with the issue is to know that the issue exists in the first place. Once that has been established it should be quite clear to the parties at risk that it is incumbent upon them to take protective measures.

The convenient thing about the physical risk is that it doesn't really matter if the cut is caused intentionally, or accidentally. Either way, if it happens you are down. The only difference between the two causes would be probability. If the probability of a cut is low then maybe you weigh the risk and potential loss verses what it would cost to be redundant and protected. It is the same concept as insurance. Having no protection is not advisable and of course there is always Murphy's Law to contend with. But one thing is guaranteed 100 percent: If you don't know the physical fiber path of your network today then you don't know your level of risk.

Hunter Newby is chief strategy officer of telx. He can be reached at hnewby@telx.com.