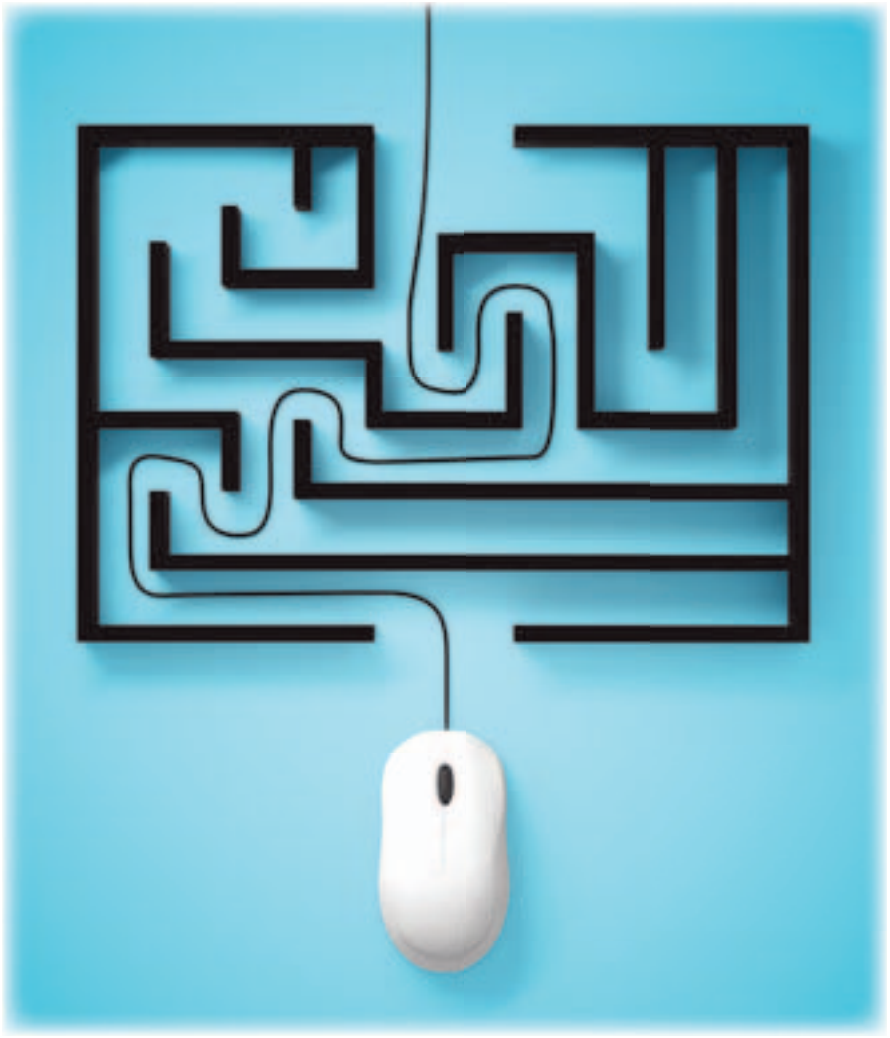
Navigating the Network Security Labyrinth

Steps to making progress on the road to network security.

By Joel Dolisy



Network security is a hot topic in all sectors of education administration. No network is immune to potential threats.

But ensuring true network protection is no small feat. Where to begin to navigate the challenges of the network labyrinth can be perplexing for even the most seasoned information technology (IT) professionals.

There is help—a road map of sorts—to ensure that your district can tackle this monolithic maze. The following simple steps can help protect the network and can provide education leaders with peace of mind knowing that their organization is taking the right path to success.

1. Standardize your network. Like a maze with multiple dead-ends, a nonstandardized infrastructure greatly increases the complexity of monitoring and managing the network, particularly when it comes to security. That complexity can increase the potential for network downtime and security breaches. Network standardization also makes it easier and more efficient to update the infrastructure.

2. Establish a clear change control process. It's all about checks and balances. Any changes introduced into an IT system must be done in a controlled manner to reduce errors. Administrators must ensure that changes to the network are made under supervision and with approval. This approach also enables real-time tracking of unauthorized changes to the system.

Don't change course for the sake of changing course. Today's networks are complex. Changing one part of the network can inadvertently affect other parts. That factor is becoming increasingly problematic as more institutions build their IT framework on app stacks, which create an interconnected maze of applications that are heavily dependent on one another—a labyrinth within the labyrinth.

Overall, having a clear change control process will ensure that your network remains on course. A lack of such control affects not only the security of the network, but also capacity planning, cost forecasting, business risk assessments, and more.

Don't change course for the sake of changing course. Today's networks are complex. Changing one part of the network can inadvertently affect other parts.

3. Implement compliance awareness standards. Compliance standards aren't just for healthcare and financial institutions. Although those industries are all highly regulated, everyone—even those in education—can benefit from their stringent measures to keep security as highly regarded as possible.

In other words, don't let security become an ad hoc way of thinking; approach it diligently. If your system doesn't already have compliance processes in place, establish them. Having clear policies and standards will help prevent security breaches. However, such policies will need adjustment and modification as technology evolves.

Avoiding Road Blocks

Now that we've discussed some simple steps that can help you navigate the maze of IT security, how can you avoid hitting dead-ends? Every good maze has its obstacles and dead-ends. How can districts avoid mishaps and road blocks?

1. Don't operate under the mantra "if it ain't broke, don't fix it." That is a sure way to hit a roadblock head-on. Even if all seems to be going well, a regular inventory of your network will reveal potential vulnerabilities so you can resolve them before a breach happens or react to them quickly in the case of a potential threat. Use network monitoring software to scan for potential vulnerabilities and receive automated alerts when those vulnerabilities are identified. Many of today's tools are self-healing and automatically repair damages.

In today's complex IT world, there will always be new threats to security and new viruses to thwart. Taking a proactive approach to ensure that the route is clear will surely bolster the security of your network.

2. Don't use outdated technology. If you're working from an outdated map, you may forever be lost in the maze! Likewise, neglecting to maintain updated security technology and device firmware opens your network to attack. Unfortunately, use of outdated technology, insecure protocols, or outdated device firmware is common. Avoid this pitfall by frequently updating your software to include the latest virus-scanning and firewall tools.

Use network monitoring software to scan for potential vulnerabilities and receive automated alerts when those vulnerabilities are identified.

3. Don't ignore BYOD (bring your own device). Consider this: in the past year, smartphone usage was up 394% and tablet usage was up 1,721%, according to Internet analytics company comScore's "2015 U.S. Digital Future in Focus" report. And more than 75% of all Americans over age 18 who use the Internet now access digital content on mobile devices, an increase of 68% over last year.

With this proliferation of use, an abundance of personal devices are connecting to today's networks—smartphones, smart watches, fitness trackers, wearable devices, and tablets. It's almost like a maze whose pathway keeps shifting.

To address this added layer of complexity head-on, track and manage IP addresses and monitor the resources those devices are accessing. User device-tracking solutions can do that by scanning your network for "rogue" or unauthorized devices that could pose a threat. In this case, it's all about diligence. Any organization must be on the lookout for potential anomalies and impending threats that could signal a data breach or an attack.

On the Right Path

Although all of these do's and don'ts of maintaining network security may have your head spinning, bear in mind that there are ways to navigate this network security maze. By following the steps outlined above, you will have your IT infrastructure on the right path to ensure that your network is as safe and secure as it can be.

Joel Dolisy is the chief information officer at SolarWinds, an IT management company. Email: joel.dolisy@solarwinds.com