Identifying, Shaping, & Meeting Team IT Needs

President, Ministry Business Services, Inc.

Reprinted from *MinistryTech*

A church IT forum discussion came up recently that is worth thinking through. The original post asked for input on how to keep team members from connecting their personal devices to the password-protected staff WiFi. The discussion that followed was a little like Mr. Toad's Wild Ride! Lots of ideas being tossed around, most of which uncomfortably avoided the most important questions.

Underlying Risk

The vast majority tried to help by explaining various ways the team could be controlled or prohibited from attaching their personal devices to the staff WiFi. There were a couple voices of reason that participated, suggesting positive ways forward.

Those not in IT may not understand the underlying risk. *Why shouldn't team members connect their personal devices to the staff WiFi?* There are legitimate dangers associated with letting personal devices attach to the staff WiFi.

- The staff WiFi, usually password protected, is typically configured to give devices full access to the organization's network as though they were connected and logged in via an Ethernet cable. That is in contrast to the public *guest* WiFi, which is typically configured to give devices access only to the internet, and hopefully access that is filtered.
- The organization's data needs to be protected. Churches and ministries maintain a lot of sensitive data that could hurt congregants and team members if not adequately protected. Data like contributions records, HR records, social security numbers of staff and some vendors, church member disciplinary notes, board minutes, and more. That data needs to be kept private, but it also needs to be kept available for team members to use in the operations of the organization. Malware like ransomware exists because hooligans understand the value associated with appropriate data access, and endeavors to block access to the data unless a ransom is paid.
- The organization's systems need to be protected. There are some who would like to disrupt the flow of church and ministry operations by crashing the system or participating in activities that could cause authorities to remove all computers and servers for forensic investigation and, possibly, evidence in a prosecution.

When team members use the staff WiFi on their personal devices, the organization's data and systems are put at risk.

The Next Question

So, does that mean team members should not use the staff WiFi for their personal devices? Maybe; it depends on why they need it.

One of the forum participants, Jason Powell at Granger Community Church, contributed "Figure out what need they're trying to solve. It took a while for our staff to be coached that there is no speed difference between our staff and public WiFi. After asking why they wanted a personal device on the staff WiFi, in almost every case, it was because they assumed it gave them something that the public WiFi didn't. A simple conversation assured them that the public WiFi would do everything they were asking for."

What if the need is legitimate, though? Jason continued, "For legit needs like interns, volunteers, etc needing a personal device to have more access, build a simple BYOD network." A BYOD (Bring Your Own Device) network is not difficult or costly to do. The cost factors involved are more to create systems that can enforce protections and recover from breaches in case they occur.

Who Decides What IT Needs are Legitimate?

This is the part often overlooked. IT is not responsible for determining what access needs are legitimate or not; that is leadership's responsibility. IT should communicate the benefits, risks, and any mitigation costs to leadership and ask for direction. Only leadership is responsible for determining who should and who should not have access to systems and data. IT's role is to engineer and configure, train, monitor, and enforce the decisions made by leadership.

Effects of IT Setting Policy

When IT makes decisions without leadership's direction, those decisions usually take the form of policies and system settings that frustrate team members. In organizations where that is the case, IT often becomes the "No" people. Some church and ministry teams get dysfunctional in the wake of those policies. Team members—who feel called by God to fulfill their ministry call—often take the posture of doing whatever it takes to fulfill their call even if it means going around IT's policies and system settings.

Effects of Leadership Setting Policy

Policies set by leadership are ultimately enforced or modified by leadership. IT has the potential of having a ministry-facilitating impact by letting leadership set policy. And leadership should fully fund whatever is required by the policy decisions it makes, which means that IT doesn't have to try to string together inadequate strategies. If leadership doesn't fund IT with what is needed, IT should let leadership know and ask for either a change in policy or a change in the budget.

Nick Nicholaou is author of *Church IT: Strategies and Solutions* and is president of MBS, an IT consulting firm specializing in church and ministry computer networks, VoIP, and private cloud hosted services. You can reach Nick at nickn@mbsinc.com, and may want to check out his firm's website (www.mbsinc.com) and his blog at https://ministry-it.blogspot.com/.