MSP 360°
WEBINAR SERIES

LabTech Best Practices: Evolving Your IT Services Offering in a Modern Mobile World

Nehring Technology, a managed service provider (MSP) based in Stephenville, Texas, has been providing business technology solutions since 2006. In this article, learn why Nehring added mobile device management to their managed services and how they are meeting the mobile needs of their clients through service and solution oriented best practices.

Modern IT Services: A Result of the Work/Life Blur

These days, everyone has a "smart" something to give them easy access to data whenever they need it. This ease of access has blurred the line between work and life; employees now have the ability to work from anywhere at any time. What started as workers simply accessing their corporate email on their phones has turned into every type of business using mobile devices for mainstream communications, developing line of business applications, and much more.

As a LabTech partner, Nehring Technology knew the benefits of using remote monitoring and management (RMM) to provide proactive managed IT services to their clients. When they noticed the proliferation of mobile devices in the workplace, they quickly realized they weren't truly servicing all of the devices connecting to their clients' networks and decided to add mobile device management (MDM) to their services offering.

However, what many IT service providers may not realize is that the uptick in the use of mobile devices in the workplace has caused more than merely a need for service. Now, security has become a necessity to protect the sensitive data stored on and accessed through mobile devices.

Breaking Down the BYOD Risk

The Bring Your Own Device (BYOD) model has become increasingly popular with many companies. As such, the need for MDM grows exponentially as a result of the high risks associated with unsecured mobile devices

connecting to corporate networks. There are three key risks of BYOD: data leakage, credibility and regulatory compliance.

Data Leakage

Unsecured mobile devices make it very easy for data to be stolen. Imagine if the president of one of the companies that you service leaves his mobile device at Starbucks. Ideally, the barista would pick it up and hold it in a safe place. But other patrons have the opportunity to pick up the device, look through contacts and perhaps even sell that information.

In addition to contact information, there is a massive amount of other confidential information stored on mobile devices, such as email attachments that might contain financial data, proprietary product details or even sensitive human resources information. In the wrong hands, this information could destroy a company.

Credibility

If malicious activity happens on BYOD devices, the damage to a company's reputation could be immense. In the age of social media, sensitive information can spread like wildfire via blog, Facebook, Twitter or other social media sites. Even with the latest Apple iOS® or Google Android™ software, people can find security exploits that open the door for extracting information.

Because Android is in a largely unregulated business in terms of OS, there are a lot of people rooting devices and getting access to unprotected layers. There is also the ability to create apps that could essentially be a virus that uploads information stored on the mobile device to spammers. The bottom line is that a person accessing corporate resources on their mobile device has the ability to damage the company's credibility and reputation.

Regulatory Compliance

MDM can help meet regulatory standards, particularly in the healthcare sector. In the past 10 or 20 years, many new bills have been passed, such as HIPPA, the Health Information Technology for Economic and Clinical Health (HITECH) Act and Sarbanes-Oxley. IT service providers can use MDM to help their clients in the medical and financial industries meet the standards and compliance requirements defined by those laws and regulations. Most regulatory compliance can be boiled down to security. For instance, do you have a password? Is that password complex? Does the password cycle in and out? If an organization is audited, such as a medical clinic, and an auditor finds that the company's iPads aren't in compliance with current regulations, the fine for each device could total more than one million dollars. It's not something to take lightly. It is critical to ensure these devices are secure.

The Benefits of Mobile Device Management

Because tablets, smartphones and other mobile devices are here to stay, managed service providers (MSPs) and other IT service professionals have the opportunity to offer a new level of service through MDM.

It's also important for clients to consider security regulations. Remind clients that if their employees are going to access company email or other confidential company information on their mobile devices, they really need a passcode on it. Security should mimic what is done in domain environments. Discuss visibility and which apps are running on particular devices, as well as what version of the iOS or Android platform is running. This vital information helps you as an IT service provider better collaborate with your clients in an effort to offer the right MDM services and ensure the proper security policies are in place.

Selling MDM to the End-User

Many businesses still do not see a need for MDM services, so it is up to you as their trusted service provider to provide content and assets to demonstrate the risks, as well as give live demonstrations of what MDM can do. Showing your clients that MDM is about security and service is critical to closing the sale. It's also important to convey to clients that MDM is not spying; it's a safety net should there be a security breach.

In addition, if your technicians are carrying around iPads or other mobile devices, make sure they are secured through MDM. If clients know that your technicians' mobile devices are being secured using the same MDM solution, it increases trust and demonstrates an endorsement of the product.

For a more detailed description of Nehring Technology's MDM experience and to see a demo of LabTech MDM, view Episode 15 of the MSP:360° Webinar Series at www.LabTechSoftware.com/MSP360.