Reassess your IT

Shore up potential IT risks created by the shift to remote work

INTERVIEWED BY ADAM BURROUGHS

Eric Thal
Managed Services Manager
Blue Technologies

216.271.4800 ext. 2636
ethal@btohio.com

WEBSITE: Don't let your shift to remote work create costly vulnerabilities. Protect yourself with managed IT services btohio.com/managed-it-services.

Managed IT service providers are busier than ever. The massive shift to remote work has exposed significant areas for improvement within companies' infrastructure and IT policies. These providers are helping companies address those issues and concerns so that businesses can continue to operate securely and productively.

"There were a lot of risks exposed as many people worked from home these last few months," says Eric Thal, managed services manager at Blue Technologies. "Businesses need to work quickly, leveraging IT specialists, to update their IT policies and procedures or develop new ones entirely."

Smart Business spoke with Thal about how managed service providers can help companies patch IT vulnerabilities as companies adjust to a "new normal."

WHAT ARE COMPANIES' MAIN IT CONCERNS RIGHT NOW?

Companies are looking for consistent and qualified IT support. They want to be sure that if an issue arises, critical or otherwise, someone can respond quickly. That's been the case as concern grows over securing networks and devices as more employees work remote. There are new questions about firewall configurations, whether VPNs are set up appropriately and if corporate data is being transmitted and stored securely.

Before the pandemic, less than five percent of the workforce had the option to work from home. There are now estimates that anywhere between 15 to 30 percent of the workforce could have a work-from-home option going forward. As remote work becomes more commonplace, there will be an increased need to address the IT processes and risks posed by that shift.

WHAT LIABILITY ISSUES SHOULD COMPANIES LOOK INTO?

With the work-from-home shift, many organizations had to scramble to purchase new laptops, tablets, or additional equipment and collaboration tools for their workers. That's because, in many cases, most or all employees were working on desktops and used to being in the office with their colleagues. These organizations had to deal with delays in getting this new equipment out to their workforce fully provisioned and secure. The delay created liability for these organizations because many of the employees, in the interim, used their personal devices for work.

This liability issue can be mitigated by deploying mobile device management. Whether the device is company-issued or personal, an MDM tool can secure and contain corporate data at each end point. In the event that a device is lost or stolen, it can be remotely locked and wiped so that no one can access the corporate data. If it's a personal device, mobile device management can keep all corporate data separate from the user's personal data, which means if the device has to be remotely locked and wiped, none of the personal information is affected.

Also, it is important to note that managed service providers can help eliminate delays in procuring new equipment because they maintain an inventory of IT assets that can be loaned to businesses until they are able to receive their new equipment.

WHAT SHOULD COMPANIES TALK ABOUT WITH THEIR IT PROVIDERS?

The most important conversation to have is about ensuring the remote workforce can access the network and critical data of the organization securely. There should also be updates to work-from-home and acceptable usage policies.

Managed service providers can help with security training for employees. Security awareness training covers the basics through the most advanced, such as how to identify a phishing email and proper data handling procedures. Employees are often a gateway into an organization's network, so this training, or at least a refresher given because of the significant changes to typical routines, can go a long way toward bolstering security.

It is always a good time to do an IT infrastructure assessment to see what gaps might exist in the environment. Pre-pandemic assessments are no longer valid because work-from-home has created additional exposure, so it's important to reassess what's going on in the environment, check for new vulnerabilities and remediate. This will help give companies peace of mind as more employees return to work and adjust to the new normal. ●