3 Problems IT Leaders Must Address Before and After Work-From-Home

Within days and weeks, enterprise organizations were forced to send hundreds of employees to work-from-home who were previously not set up to do so.

This included finance, HR, marketing, executives, and more people who all need different levels of access and security.

In this article, MDSi explains the common network and security issues that arise when making quick decisions.

How do they identify and fix any design gaps before a disaster, like a security breach, occurs?

Continue reading to learn the main problems IT leaders must address before and after work-from-home.

You were going about your responsibilities as an IT leader for your enterprise organization, keeping the network up and secure while planning for the future.

Then, the 2020 COVID-19 pandemic hits.

Within days, you needed to hundreds of employees to work and access company data from home who were not previously set up to so. This included finance, HR, marketing, executives, and more people who all need different levels of access and security.

Your responsibility was to make this happen in a safe and secure workflow so intellectual property didn't escape the company, especially during a fast adjustment. You have to do this in a way that doesn't kill the bank but still keeps the business alive and production facilities moving.

We're now more than half a year into the 2020 work-from-home era, and many companies are still making the transition on how to accomplish work-from-home in a safe, secure way.

At MDSi, we're talking to many IT leaders who made these IT and security decisions within weeks, some within days. They're asking if they made the right initial decisions and if they are still making the right decisions. How do they identify and fix any design gaps before a disaster, like a security breach, occurs?

As an advisor to these IT leaders, I'm working with them to ask the right questions and solve for the right problems within their unique business.

To make this process less daunting, we categorized three main problems every enterprises IT leader needs to solve:

- How do you expand connectivity and capacity?
- How do you secure it?
- How do you bring the workforce back on site?

In this article, I'm sharing how to think through each of these problems and key questions to answer.

Expanding for Remote Capacity and Connection

The strategy for expanding remote capacity and connection is different for each organization. Factors such as the industry, data type, technology stack, budget, and future strategy all play a role in how to allow for a remote workforce.

It not as simple as adding five boxes here and another five boxes there. It's also about making sure we make the most of the infrastructure and can actually secure the network once it's expanded.

Start by asking questions like:

What does your company's current remote work force look like? What are your challenges with this remote workforce? Are your users happy? What are the most common performance issues?

What do you have in your existing infrastructure? What is your inventory? What is your workflow?

Where do your applications and data live? If all of your databases are local, such as a local server at your facility, then we have to do some sort of remote connectivity or VPN. If everything is cloud-written already, then you're more prepared for a remote workforce. We may just need to change some access control rules.

How much data is sensitive? Who needs access to which data? Can we make sure that everyone has equal access to applications and still access their existing data as well? Some organizations can't send much of their data to the cloud because of the amount of sensitive data that would be unsecured or less secure in a cloud infrastructure than on premise.

Expanding Network Security

There is a larger surface area as the network expanded into hundreds of employee homes. This means there is more potential for vulnerabilities and security holes. In the rush to get employees working from home, we've seen that people made a lot of quick decisions that may not be in the best interest of protecting intellectual property.

We like walk backwards to make sure that we understand the whole solution. This helps us present a strategy and design that's going to accomplish the enterprise's goals and keep it secure.

Now that you've scaled, how you can you be sure this is secure? For example, the initial answer may be to add 500 VPN licenses and duplicate the configuration. But, if there were even a small error in that initial configuration, this could lead to a significate security issue.

Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
p +1 408 745 2000

MDSi
6225 Shiloh Rd.
Alpharetta, GA 30005
p +1 800-874-9850

How do your decisions impact the performance of the network? It's common for security measures to hinder network performance, but it doesn't have to. Are you gathering network performance data? If so, how? How are you monitoring and interpreting that data?

We've seen many IT teams start gathering this performance data but not understand how to relate it to make sense of how users experience the network.

Returning On-Site

The most forgotten yet critical questions to ask for preparing a long-term strategy include how, and if, to bring the workforce back on site.

Will everyone come back to the office? Many organizations are transitioning to have a more permanent workforce. How much of your workforce will stay remote, come back on site, or be a combination of both?

What will you do with the infrastructure? It's likely that security issues will rise unless there is a developed plan to bring infrastructure back in house.

How do you plan to bring capacity back on-premise? Many enterprises turned on a lot of cloud-based applications and SaaS like Zoom, Office 365, and more that made working from home easier. This means a lot of demand on the ISP and the broadband has been deferred to employees' home networks. But, they're going to be putting that additional capacity and demand on the enterprise network production network when employees come back on-site.

This may cause performance issues for when people come back and continue to use these applications. Performance may even be worse in the office than it is at home.

How will you monitor shadow solutions? You're likely going to have this backlash of people who have developed shadow IT solutions. Take for example employees using service-type solutions for collaboration, storage, file share, and more that people may have started using that weren't officially sanctioned by IT.

When employees come back and continue to use these applications, you're now using an unsupported platform with possible security complications/ applications.

You can help prevent these shadow IT issues from happening if you're using something like Juniper's security solution because of the layer seven application security. Otherwise, you'll need additional (and often manual) management to identify which applications may be causing a threat to your organization.

Conclusion

Fortunately, solving for this third problem of bringing the workforce back on site is much more simple once challenges of expanding connection and security are solved.

That's why it's so critical that IT leaders build their team with the right expertise. Asking the right questions in the beginning and throughout design and implementation will help make sure you're as agile and secure as possible.

Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
p +1 408 745 2000

MDSi
6225 Shiloh Rd.
Alpharetta, GA 30005
p +1 800-874-9850

Next Steps

Wondering if your organization's network has the agility, security, and strategy for whatever the market demands next?

Reach out to MDSi for help with your IT network and security strategy design and implementation.

You can also get to know us better by following us on LinkedIn.

Stay tuned. We're sharing more stories and insights that will be published on the News section of our website.

Coming Up

In our next article, we're sharing a story of how one MDSi partner designed IT and security plans for multiple enterprises that were scrambling to send hundreds of employees to work-from-home.

Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
p +1 408 745 2000

MDSi
6225 Shiloh Rd.
Alpharetta, GA 30005
p +1 800-874-9850

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701