NFINIT

COVID-19 Related IT Issues

and Why the Biggest Challenge is Yet to Come

Introduction

COVID-19 has brought societal and economic upheaval unlike anything we have seen or likely ever will see again. The pivotal event has transformed how we live, interact, and work.

Due to the pandemic, an incredible **42% of the U.S. labor force is now working from home** full-time. With COVID fewer people are working in corporate offices and this trend could remain for the indefinite future. As a direct result of this global health crisis, **25-30% of the workforce will be working from home** multiple days per week by the end of 2021.

The increased numbers of employees working remotely combined with high unemployment rates are forcing companies to **downsize office space and rethink how and where they manage IT infrastructure.** Never before have corporate real estate and IT strategies been so intricately linked.

Home-based employees and BYODs have limited security controls elevating security risk for the corporate networks and centralized data centers they run through. What can be done to **bolster cyber defenses** now that a large percentage of the workforce is working remotely?

Where Does this Leave IT?

Few areas of business have escaped this catastrophe unscathed, and IT departments are no exception. The transition to working remotely — amongst other factors — has made it far more challenging for IT departments to help businesses maintain their technological efficiency and overall productivity.

Even if you haven't yet noticed it, the aftershocks of this tectonic shift towards a decentralized work approach will be felt for months, if not years.

> To prepare for what's to come, your business must not only anticipate these obstacles but preemptively act to mitigate them.

Below, we'll discuss the four most pressing challenges IT departments have yet to face, and then prescribe countermeasures you can take to get ahead of the curve.

COVID-19 Related IT Issues and Why the Biggest Challenge is Yet to Come

Before everything was flipped upside down, businesses faced significant IT obstacles. From security to support to infrastructure, these were difficult enough tasks to handle back then. Plus, matters were further complicated by the fact that many of these challenges were evolving alongside technology — like a proverbial whack-a-mole, for every problem that was fixed, a new one cropped up.

Staying atop things was a formidable test for just about any IT department. But in the wake of COVID-19 and the work-from-home approach, the difficulty level switched from “normal” to “nightmare” in a snap of the fingers. For example, security was already a weighty concern for most businesses, but now, remote work creates new problems.

Suddenly, you’re faced with curveballs like:

- What do you do about occupations that are highly regulated, utilize proprietary legacy software systems, or that require heightened security?
- How do you ensure that software is optimized and properly patched for remote work?
- Will normal home networking infrastructure be able to handle bandwidth without breaking?
- For employees using personal computers and devices, how can you prevent viruses or malware from entering through unvetted machines into the core network?

This barely scratches the surface of the security concerns, let alone the various other responsibilities an IT department manages. Put simply, this is an unprecedented time. We're in uncharted waters.

Unfortunately, we're just getting started — the worst is still yet to come.

That is, unless you take the time to understand the landscape, prepare for the challenges, and implement **the right solutions** before things get out of hand. But what are they?

Compute Resources

With both the global supply chain and public cloud resources significantly impacted, such changes beg the question, **"Are you prepared to stay agile though these circumstances?"**

As the initial transition from the office to home took place, IT departments did the best they could to build a patchwork of systems and remote offices fit for handling the rigors and demands of work. But, because these setups are a temporary fix, it's anticipated that the decoupling of applications and desktop compute environments will create unintended consequences, highlighting previously unknown dependencies and creating additional stressors. As a result, future challenges NFINIT anticipates include:

File level access issues

Users that once had file access through a shared network folder, will no longer be able to do so. This will add a further element of complexity around collaboration and sharing, particularly for larger files like CAD, PSB, and multimedia files.

Application and end-user distancing

Many apps will experience performance issues due to the latency between the workstation and the backend applications. This issue will be heightened as the app runs through unpredictable and oversaturated residential networks.

Compute infrastructure availability

Due to the negative impact on global IT supply chains, acquiring the necessary infrastructure becomes an even greater headache. In many cases, you simply can't say whether the supply will increase or when a needed piece might arrive.

Remote data center management

While most organizations have some remote-monitoring tools, few have a complete portfolio that's not only in place but tried and tested. As a result, in-house data centers and their underlying infrastructure are at risk and IT response times will be impacted.

Public cloud resource contention

As global supply chains are constrained and public cloud experiences a rapid migration of workloads, capacity constraints loom on the horizon.

Total Cost of Ownership (TCO)

Companies will be forced to prioritize their IT spend and reevaluate their approach. Risky expeditious plans will fall by the wayside in favor of safer, more thoroughly researched projects.

Network Impact

As workers have moved into home offices, network requirements have changed. From subpar home internet, to a lack of network resources, to the inability to transfer large files, a growing number of companies will soon realize that they lack all of the requisite pieces for a flawless transition. Expected impacts to networks include:

Extension of the status quo

In the early phases of the work from home (WFH) movement, IT administrators initially attempted to simply “extend the network” by letting users access the office network via VPN. But this opens up a whole new can of worms, leading to questions like:

- Do users have the proper devices and bandwidth at home and will the existing equipment be capable of handling the load?
- How can network administrators address security concerns, especially with all of the necessary concessions and laxening of normal security protocols?
- How can IT departments provide remote support to non-technical users or those that are barred from using their own device?

Home network optimization

Even in the best of times, home networks’ capacity and bandwidth is often inadequate. But with all of the additional WFH traffic, local ISP and WiFi hubs can expect slowdowns and outages.

Scaling connectivity at the HQ or data center

Traffic that once was channeled through local LAN or metro-e links is now being sent over the internet, which raises two questions:

- Is there enough bandwidth to handle the load?
- Is the configuration sufficiently reliable?

These sudden changes will force IT departments to examine their networks and network capacity in an entirely new light. As both technical and financial resources shift, cost optimization will become necessary in order to weather the gathering storm.

Security

The combination of home-based networks and employee-owned devices — both with limited security controls — constitute a security risk to the corporate networks and centralized data centers they run through. What must be done to maintain a vigilant watch and ensure that intruders don't breach your cyber defenses?

Security concerns are not only the single largest risk factor of COVID-19, but will also have a lasting impact far into the future. As IT teams scramble to set up improvised home offices, cyber thieves are also rushing to exploit vulnerabilities in these makeshift systems. Thus far, we've already witnessed a notable uptick in the frequency and the sophistication of these cyber attacks. With this in mind, further IT security challenges businesses face include:

BYOD

As employees work from home on their own devices, companies must figure out ways to prevent these personal devices from becoming security gaps. From lack of anti-virus protection to improper online, social media, and email practices, employees who work at home represent a sizable security risk. This is magnified by the fact that many users are more relaxed and less wary about potential intrusions when they're out of the office. They are more likely to click on an email

or link that claims to provide information about COVID-19, only to discover that it contains malware or a virus.

Training and testing workers

IT departments have to brainstorm ways to train end-users remotely. But due to the sheer number of risks, covering all of the bases poses a considerable obstacle. From there, IT teams must formulate an effective testing methodology that accurately gauges the success of security training.

Access to corporate networks and data

The move from the workplace to the living room has added an additional layer of complexity to the challenge of protecting corporate data. Companies will be faced with the choice of turning to VPN and/or data encryption to reduce risk to sensitive data.

Home office security gaps

Most home networks and residential routers are woefully inadequate in terms of security. This will force IT departments to create a new security perimeter, using modern approaches to endpoint security such as:

- Signature based protection
- Machine-learning based protection
- Ransomware protection
- Data loss prevention
- File integrity monitoring
- Network based protections
- Out of office software updates
- Centralized reporting and management

Business Continuity

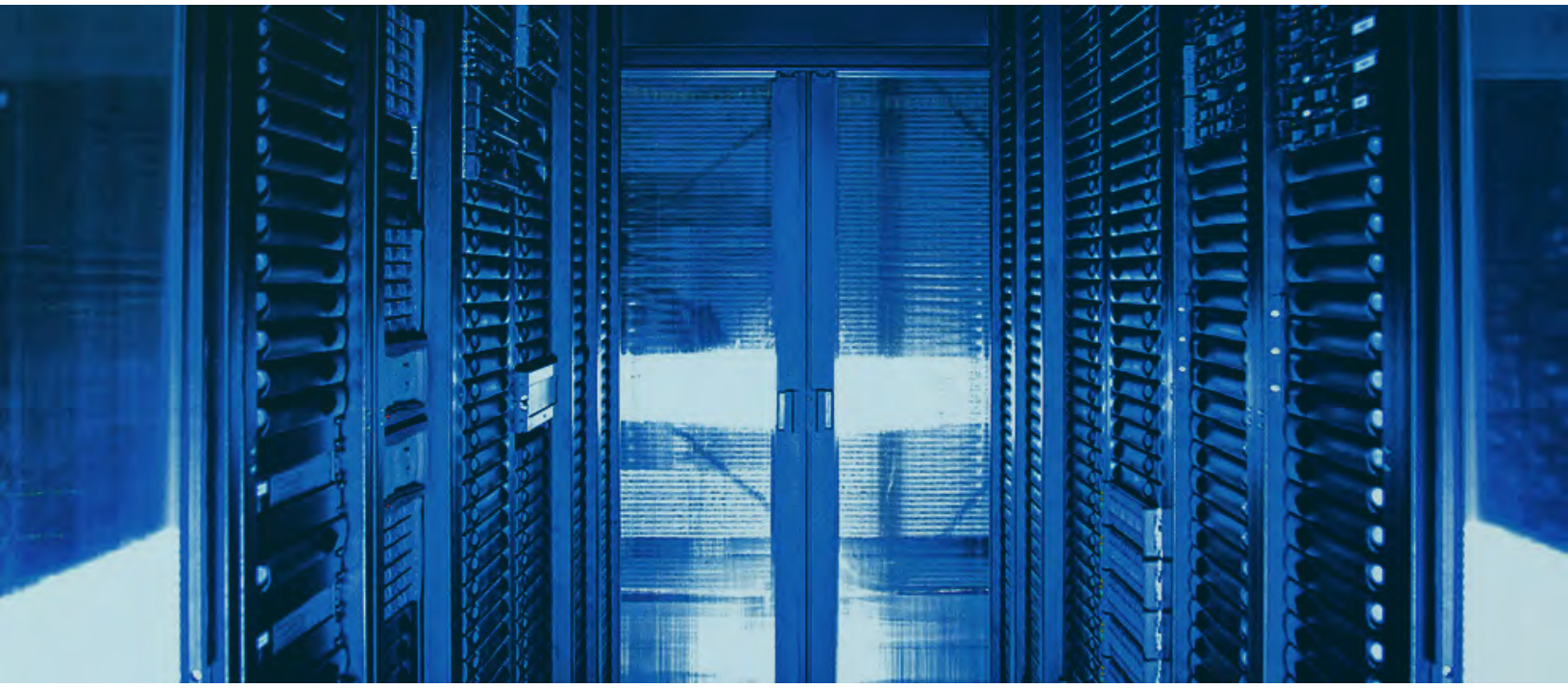
With most companies experiencing unprecedented demands on internal IT resources — both infrastructure and human labor — how do you plan on returning to business as usual?

As companies emerge from the Coronavirus, there will likely be a mad scramble as companies jostle to stake their claim in the post pandemic world. To take advantage of the opportunity, businesses will require customizable solutions that ensure uptime of vital applications and reduce the costs of an intrusion or unplanned outage.

Even after COVID, business continuity will still present a challenge, since disasters of all shapes and sizes are an inevitability. From human error to system failures, businesses require technology and processes that mitigate or eliminate threats.

But you can't stop there.

> After disaster strikes, businesses ought to have strategies in place that help it stay operational and then fully recover in spite of obstacles or hold-ups.



The Solutions to COVID-19 Related IT Challenges

So, what can be done about these serious IT issues? How do you ensure that these issues are only speed bumps and not barriers to your operations?

While the answer to that question will naturally depend upon your business' applications and IT infrastructure, NFINIT regularly utilizes three primary solutions to solve these problems:

Cloud hosting and migration

Cloud technology diminishes the severity of many of the challenges discussed above. It increases a company's flexibility, allowing employees to work from anywhere. The cloud provides a safe way to virtually access the same files, apps, and resources that they would have in the office. And due to the scalability of cloud services, cloud hosting and computing can accommodate significant influxes of remote workers.

> With NFINIT cloud services, you can meet your scalability, resiliency, and security requirements without sacrificing speed and power.

Services include:

- Community cloud
- Private cloud
- Public cloud
- Storage as a Service (STaaS)

Network Services

NFINIT's team, tech, and processes can be used to support any business' integrated network infrastructure. From the outset, NFINIT designs, implements, and then manages a custom network that is both secure, reliable, and usable whenever, wherever.

Tools used to achieve this include:

- **Advanced internet service** – Multiple carriers over one connection for high-speed connectivity.
- **NFINIT network passport** –Aggregate all of the ever-changing endpoint requirements created via a hybrid multi-cloud IT strategy.
- **DDoS mitigation service** – Next-generation user ID tools and tech help your network or application resist any type, size, or duration of DDoS attack.
- **Managed endpoints** – Active monitoring, management, and security tools help businesses protect their network endpoints.

Data Center Services

Especially when your team is out of office, you require a reliable data center to host all of your critical data and systems. NFINIT offers secure, high-performance data centers for all of the vital IT deployments, freeing you from the costs and obligations of maintaining that infrastructure on your own.

Data center services include:

- Carrier neutral colocation
- Managed colocation
- Structured cabling
- Outsourced operations

Security Services

Take comfort knowing that you're properly protected, whether your users are working on enterprise or BYO devices.

NFINIT services provide the following benefits:

- Endpoint protection with artificial intelligence
- Firewall with synchronized security built in
  - IPS/IDS
  - WAF
  - SSL VPN
  - URL Filtering
- 24/7 threat hunting, detection and response
- Public cloud visibility and threat response
- Centralized management, auditing and logging
- Security Awareness
  - User security training with quantifiable reporting
  - Sample email phishing campaigns with credential harvesting or attachment based attacks

Business Continuity Services

NFINIT takes a unique approach to working with clients to understand their business requirements and then designing a comprehensive plan to meet the RTO and RPO requirements defined.

This allows for companies to map to the appropriate investment to the required level of redundancy on an application by application basis.

- **Disaster Recovery as a service (DRaaS)**

  We combine the data replication, cloud platform, network, and endpoint management to create a complete DRaaS 360 service, which has you covered from endpoint to application.

- **Back-up as a Service (BaaS)**

  NFINIT can holistically provide the service for you, or you can seamlessly connect to NFINIT as a remote storage solution, providing the required infrastructure and network components for a secondary offsite backup target.

NFINIT—Your Trusted IT Partner During and After COVID-19

In the wake of COVID-19, the IT threat landscape is rapidly changing by the day. To not only prepare for (but get ahead of) these mounting challenges, it's vital that you partner with a technology services expert that can assess your IT infrastructure and applications, identify your weak points, and then suggest prescriptive actions.

As the leading provider of enterprise-class cloud, connectivity, colocation, and technology services, NFINIT has worked with scores of clients, helping them navigate these perilous times. Rest assured, we can help you too. Our seasoned team of experts provides a unique perspective and all of the resources you need to enact your current and future IT goals.

Don't wait for an IT meltdown, network interruption, or cyber breach to alert you of security and network issues.

Take the proactive road and turn to our team of dedicated experts!

CONTACT US