Integris.

Your Modern Workplace Journey

A Business Leader's Guide to Sustaining a Remote Workforce for the Long Haul

integrisit.com

A Business Leader’s Guide to Sustaining A Remote Workplace for the Long Haul

Today’s modern workplace looks quite different from how we envisioned it just a year ago. Many organizations are finding themselves struggling to transition to a new playing field, full of remote workers and unforeseen challenges.

When the shift to remote work first started, you scrambled to get operations moved from the office to home. Since then, the nature of work has changed. You have found that your employees, now that they are settled into this new working situation, find themselves enriched and fulfilled. This makes the quality of their work much higher and they feel happier, more valued, and more likely to stay with your organization.

Your Modern Workplace Journey: A Business Leader’s Guide to Sustaining a Remote Workforce for the Long Haul will help you reimagine what the journey to a new, modern workplace could look like for you, including:

- Challenges Facing Business Leaders with a Remote Workforce
- Encouraging and Measuring Productivity of Remote Teams
- Cloud Services to Fuel Your Connectivity and Collaboration
- Cybersecurity in a Remote Environment
- Elements of a Successful Transition to a Remote Workforce
- Embracing the Human Side of the Remote Workforce
- The New Role of Managed Services Providers in a Remote Work Environment
- How a Partnership with Integris will Help You Sustain Your Remote Workforce

The Challenges

Facing Business Leaders with a Remote Workforce

You have been playing this new game long enough to realize that being successful with a remote workforce takes a lot more than sending employees home with a "to-do" list. Some of the recurring challenges facing business leaders in today's workplace include productivity and time management, budgetary considerations, connectivity and collaboration, cybersecurity, and supporting your company culture.

Productivity and Time Management

Productivity may feel like it should be a huge concern for business leaders, but statistics say that remote workers work an average of a day and a half more per month and are 47% more productive.

The ongoing challenge faced by businesses with remote workforces is measuring productivity and encouraging employees to manage their time wisely and to complete projects and tasks.

Budgetary Considerations

While setting your employees up for remote work may have initially cost businesses money for equipment and new software applications, organizations are now finding that enabling remote workers saves them money in overall spending.

The savings come from things such as lowered utility costs, decreases in office space rental fees, supplementary services such as cleaning crews and trash removal, and petty cash savings for snacks, coffee, and other breakroom/ restroom necessities.

Businesses still face budgetary challenges in the form of keeping technologies competitive. It is expected that IT budgets will remain the same or rise over the next year, with the biggest jump in IT spending focused on heightened cybersecurity. While the costs of having employees work from the office has been lowered or eliminated, these gains are offset by the need to keep remote workers equipped and working safely.

Connectivity and Collaboration

In a work-from-anywhere world, employers have been struggling to find ways to keep employees connected. Files, notes, and other data must be shared quickly and securely. Additionally, teams must be able to meet in real time, despite their geographical locations. As a result, business leaders have had to shift their mindsets from a safe and connected office network using servers to a new mindset, known as PaaS, or Platform as a Service.

PaaS and cloud computing are an excellent option for organizations, and some of the biggest names in operating systems and applications have risen to the new challenges of connecting remote workers. Microsoft is still the largest provider of cloud solutions, bringing connectivity and collaboration to teams no matter where they work, from across town to across the globe.

While cloud solutions are the best choice for being connected, many business leaders and employees alike find themselves struggling with the applications they need to use. Teams, for instance, is an excellent all-in-one solution but businesses may be hesitant to try it because it seems overwhelming. The size of the program and its many integrations and applications may prevent many organizations from really harnessing its full power.

The challenge with connectivity and collaboration isn't finding the right solutions as much as it is understanding them and using them to their full potential.

Cybersecurity

As we've already seen, businesses are shifting their IT budgets to meet the growing need for increased cybersecurity. It's no surprise that hackers are targeting remote workers and unleashing every wily weapon in their arsenals from ransomware to spoofing, phishing, and business email compromise. Many employees have smart homes connected via the Internet of Things, increasing their vulnerability. Still others may enjoy working from a local coffee shop with weak Wi-Fi security.

As the number of remote workers increases, hackers are using increasingly sophisticated attacks.
No industry is safe, and the size of your business won't protect you, either. An estimated 43% of cyberattacks target small to medium sized businesses, an increase of 424% in 2019 alone.

The challenge of cybersecurity is even greater for business leaders than ever before: how can a business secure its network when employees themselves may be engaging in risky behavior?

Support Company Culture

You have worked hard to set up a work culture that fulfills your employees, recognizes your organization's mission, and helps the public's perception of your business align with your own.

With employees scattered, it's easy to lose sight of the qualities that make your business unique. Maintaining company culture is more important now than ever before.

It's important to find ways to reinforce your company culture through team building exercises, "social" events, and fun contests.

Encouraging and Measuring

Productivity of Remote Teams

A successful remote workforce will need to have reliable solutions in place to help them stay organized, connected, and productive. Your managers will need a way to assign tasks, follow up on assignments, and measure employee productivity.

Keep Tasks in One Place

There are many software programs designed to help employees prioritize tasks. The important thing is to make sure all assignments are in one place, streamlined and prioritized for your remote workforce.

1. **Microsoft Planner** is part of the Microsoft 365 offerings and is a great way to organize tasks. Planner allows flexible task management, is fully customizable, and allows managers to assign the proper team members to each task. Files can be shared within Planner, and all notifications can be integrated into Microsoft Outlook for real time notifications.

2. **Traction Tools** is an EOS (Entrepreneurial Operating System) that allows managers to assign tasks, collaborate with team members, and follow progress on assignments. Meetings are easily planned with Traction's preset outline that covers progress reports, to-do's, and issues that need to be discussed. You can assign teams to different "workspaces" to keep employees together according to their jobs and responsibilities.

3. **Monday.com** is a program that allows managers to see the success of team projects and keep track of status changes on assignments in real-time. Employees stay on track with automated notifications for routine tasks. Due dates and priorities can be set in Monday.com, and all stages of the project are clearly marked from its assignment to its completion.

4. **Microsoft Teams** is one of the most powerful applications available to help you organize, communicate, and share files. Part of the Microsoft 365/Office 365 suite, it's a highly customizable way to keep track of your projects.

Measure Employee and Team Productivity

Your managers may need a little extra organization as they try to keep track of employee productivity. These programs are designed to give organizations a way to measure productivity for teams as well as for individual employees.

1. **Culture Amp** is a great evaluation tool that allows employees and managers to provide real-time feedback. It allows employees' skill sets to be updated and shared so managers can best understand the skills each employee brings to the team.

2. **Hubstaff** is an all-in-one product that allows managers to track employees' progress on specific tasks or measure team performance. It offers time tracking and activity rates and allows managers to see who is working in real-time. Tasks and projects can be viewed on one page to allow managers to see progress on each task as it relates to the next, allowing flexibility in assigning priorities to each task.

3. **Trakstar** is an employee productivity measurement tool that allows managers to set goals, track progress, and evaluate performance. It uses feedback from employee's peers and auto-generated reports to help give a more complete picture of the employee's work and encourages employees to self-evaluate for a better understanding of their own progress.

4. **Asana** is a one-stop shop application that allows managers to organize tasks and measure progress of individual team members as well as the entire team. Asana lets users establish goals, measure workload, build projects, and streamline with automation.

Don’t Over-Manage Your Employees

It’s tempting to think that your employees are not doing work, but the reality is that 76% of employees feel they are more productive when working remotely. It’s hard to believe, but there are less distractions for those working from home than those in the office. Less meetings, quieter workspaces, and uninterrupted work time allow remote employees to really focus on their work.

For managers, letting go is the hardest thing. Discourage your managers from having endless meetings, bombarding inboxes with constant demands, and calling employees throughout the day. If your employee was a good worker in the office environment, s/he will be equally as productive while working from home.

Other than a daily team meeting (called a Huddle or Scrum) to get employees focused on the day’s tasks, all other meetings should be kept to a minimum. More than 20% of a day spent in meetings isn’t just annoying, it is counterproductive. A once a week progress meeting should be sufficient to keep the team’s goals aligned, and an employee-manager meeting once per week should be enough to keep track of individual progress.

Cloud Services to Fuel
Your Connectivity and Collaboration

Your remote workforce will need innovative new ways to collaborate and stay connected in the modern workplace. Organizations are finding that moving to the cloud keeps teams connected and productive.

More Time, Less Headache, Lowered Costs

Cloud management brings a third-party into the organization, freeing up your workers and IT staff to work on your business' projects. By removing the responsibility of server management from your IT teams, cloud management providers give time back to them that can be spent focusing on your business. The cloud provider will take on the responsibilities of upgrades to software and hardware, IT issues, and cybersecurity.

Businesses find that using a cloud services provider allows them to decrease the workload on their own IT department and save money on the IT budget by removing the costs of servers and not having to increase their personnel to meet the IT demands of a remote workforce.

Increase Productivity and Keep the Competitive Edge

When your employees are connected and productive, your business stays competitive in the modern workforce. The cloud levels the playing field for businesses by allowing real-time work, enhanced project collaboration, and increased communication.

The cloud increases connectivity within your own organization as well as with your customers and prospective clients. From Zoom to Teams, your team can reach out to anyone, anywhere and keep your business flowing smoothly.

Increased connectivity allows your teams to share important files and data and access it anywhere they are currently calling “the office.”

Stepping into the Future

Cloud based technologies allow your business to expand across your city, your state, across the nation and globally. Increasingly, the old way of doing things is becoming obsolete; your business model must adapt, or it will be left behind. Cloud computing allows organizations to grow and reach a wider audience than ever before.

Cloud based solutions also give your organization access to cybersecurity strategies to protect itself and a responsive disaster backup and recovery system that restores your files and data far faster than older methods after an incident.

Microsoft Powers the Modern Workplace

The biggest player in the modern workforce is Microsoft 365. While many organizations use Microsoft 365 for email, they may be overlooking the other applications within this powerhouse of a cloud solution.

By far, Teams is the best multi-tasking one stop solution for remote workers, featuring:

- Instant Chat communication
- Audio and video meetings between employees, including recordings
- Customizable groups (teams) that allow your employees to streamline communications and share documents and files between other group members
- Access to shared documents in SharePoint
- Privacy setting for groups
- Ability to include outside contacts to groups
- Availability settings
- Help bots, survey bots, scheduling bots and more
- Document storage in the cloud so all team members can access them, wherever they are
- Tag notifications and team alerts
- National and global reach
- Universal accessibility

Teams is fully integrated to other Microsoft applications your business uses such as Outlook, Word, Excel, PowerPoint, and SharePoint.

Microsoft has recently upgraded its business platform from Office 365 to Microsoft 365, with all the features your business was using plus many more. If your organization hasn't explored the full Microsoft 365 suite, chances are that you aren't as connected and productive as you should be.

Hybrid Cloud Solutions

Depending on the applications your organization uses, you may not feel it's necessary to move all data to the cloud. Hybrid cloud solutions may be the right fit for your organization, but at the minimum be sure to use the cloud for:

- Email
- Shared files
- Backup and Recovery solutions
- Collaborative applications

Cybersecurity

In a Remote Environment

There is no doubt that a shift to a remote workforce has placed organizations at a bigger risk for cybercrime than ever before. Employees and management both must be aware of the potential threats that a lax attitude about security will cause. You can do a few things within your organization to lower the risks.

Limiting Administrative Privileges

Employee devices are automatically set up to recognize them as administrators. Remember that administrators can install software and allow changes to the settings on their devices. This includes things like bypassing security features or downloading unauthorized software to their devices. Security can be strengthened by allowing only a few people to have access to your network's connected device settings.

You will also want to limit application access to those who need the program to perform their job duties. No one in sales, for instance, will need access to Human Resources applications and programs, and only a select few should have access to any high-level administration programs.

By limiting your employees' access to unnecessary files and applications, you will also be limiting the amount of damage a hacker can do if s/he infiltrates the network.

Adopt Multifactor Identification Universally

Multifactor identification takes the advantage away from hackers by forcing them to have two or more levels of identification to access your network.

When equipped with multifactor identification, the user must provide “something they know,” like a password, with “something they have,” such as another device or a biometric identifier (fingerprint or voice recognition). The hacker can't finish the puzzle without all the pieces and will be unable to log onto your network.

Strict Password Requirements

Integris follows the GET STRONG approach to password creation:

- G **GO WITH ENCRYPTION:** All passwords should be stored with encryption.
- E **ESCAPE COMPLEXITY:** Even though the password rules may be complicated, try to create them so they are easily remembered.
- T **TEACH EMPLOYEES:** Make sure all employees know and follow password rules and requirements.
- S **SIZE MATTERS:** Longer passwords are harder to hack, so all passwords should be a minimum of 8 characters. System passwords should be between 12 and 50 characters in length.
- T **TRUST NO ONE:** Add authentication processes to logins, such as Google Authenticator, Duo, RADIUS tokens, or other 2-factor options.
- R **ROTATE OFTEN:** Users should change their passwords every 90-180 days.
- O **OMIT DUPLICATES:** Never use the same password across multiple applications, systems, and accounts.
- N **NO CHEATING:** Disable password hints.
- G **GET A VAULT:** Store passwords in secure vaults such as 1Password

Following these steps keeps your users safe and your network protected.

Cybersecurity Awareness Training

The fact that employees are responsible for most malicious attacks isn't surprising. Your employees are both the largest vulnerability to your network as well as one of the biggest lines of defense for your organization.

Cybersecurity Awareness Training is the first step to ensuring all employees are aware of threats, and the best way to teach them how to avoid risky behavior. Mandating cybersecurity awareness training is not only a way to decrease threats to your business, it can also help you protect your business from liability if an incident occurs. Make sure to have documentation of successful cybersecurity awareness training classes in each employee's file.

Cybersecurity awareness training should incorporate:

- Email best strategies
- Phishing simulations
- Detecting and reporting suspicious activity
- Chain of notifications for attacks
- Strategies for strong passwords
- Trending industry-specific cyber threats
- SOP (Standard Operating Procedures) for immediate actions following a suspected cyber attack

Firewalls and Antivirus

When the shift to remote work started, your business was not prepared to equip all the devices your employees were using with robust firewall and antivirus protections. Now that the modern workforce is here to stay, it's time to shore up those defenses.

Free solutions aren't the best choices for a permanent remote workforce, but they are better than nothing at all. Microsoft features Windows Security as part of its Windows 10 experience, and there are other free strategies available as well. These may be a good place to start, but you will need to upgrade your antivirus to a more rigorous strategy to keep up with today's trending cyber threats.

Artificial Intelligence is the latest trend in antivirus solutions, but AI technology alone isn't enough to protect your network. Cybercrime is ever evolving, and your antivirus must evolve as well. AI is not just for the good guys anymore; cybercriminals are using this technology, too.

Human oversight of cybersecurity strategies is what makes a paid cybersecurity platform far superior to a free version or "boxed" online solution. Cybersecurity is one aspect of your IT that is best left to the professionals who can scale protections to the level of threats your organization faces. The pros will be able to supplement antivirus solutions with human oversight, preventing an antivirus from blocking "good" applications or letting trojans disguised as "good" applications slip past.

Allowing technicians to manage your cybersecurity platforms means that they will handle routine testing, scans, event log monitoring, updates, security patches, and other mundane but necessary IT tasks.

Acceptable Use Policies

Part of your cybersecurity strategy should involve passing acceptable use policies to be followed while connected to your network, whether your employees are using their own equipment or not. Work issued equipment will have other clauses to cover the acceptable use of organizational devices.

As with cybersecurity awareness training, copies of these signed policies should remain in an employee's file to help protect your organization from liability following an incident. You can introduce acceptable use policies as part of your employee cybersecurity training so you can go over the documents thoroughly.

Backup and Recovery Plans

Backup and recovery plans are for more than cybersecurity incidents. They will help restore data quickly following any kind of disruption including natural disasters, power outages, and accidental file deletions.

Cloud solutions offer the fastest data restoration strategies, so it is highly recommended you store your backups in the cloud to minimize disruption.

On top of lost productivity and downtime, not having backup and recovery strategies can put your organization at risk for regulatory violations. Regulatory agencies are extending their reach deep into the way organizations store data, data transfer processes, and ensure privacy. HIPAA (Health Insurance Portability and Accountability), PCI, and HITECH are just a few of the governing bodies of digital business continuity.

Your backup and recovery strategies are another area that is best left to the professionals. They understand your industry's regulatory requirements and can offer the best solutions for your business to minimize disruption, lessen unplanned downtime, and lower the impact of data loss.

Virtual Private Network Usage

Your organization uses a VPN (Virtual Private Network) for its remote workforce, but that doesn't mean your employees' connections are completely secure.

VPN safety relies on people, passwords, and protocols.

- **People:** A VPN won't prevent malware and hacking if your employees are still engaging in risky behavior online or do not follow email best practices.
- **Passwords:** Your VPN security will only be as strong as the passwords your employees are using to access it.
- **Protocols:** VPN protocols are the set of rules that are used between the VPN client and the VPN server. The more stringent these protocols are, the safer your connection.

Paid VPNs tend to have more rigorous protocols and better data encryption, making them a superior choice to their free counterparts.

One final note about VPNs: Discourage your employees from using unsecured Wi-Fi connections. Your VPN alone won't be enough to protect your network if the connection is not secure to start with.

Cyber Risk Insurance

If you haven't upgraded your organization's cyber risk insurance policy, this is the time to do so. You may find your premiums will be decreased because of the extra cybersecurity precautions you are taking.

You will want to address the added cybersecurity threats, however, by increasing your policy's coverage.

Look for cyber risk insurance carriers and policies that cover (at a minimum):

- Payment of ransomware
- Data breach notifications
- Identity restoration and credit monitoring
- IT forensics
- Legal expenses
- Data restoration
- Public relations intercessions
- Income lost due to business disruption
- Legal fees secondary to breach of contract with clients
- Limited hardware replacement for devices damaged secondary to an attack

Many cyber risk insurance carriers will refuse to cover:

- Acts of war
- Future profit loss
- Claims for replacement of remote equipment or personal devices
- The costs of upgrading technologies

Your organization will have the best chance of paying lower premiums and deductibles if all employees undergo cybersecurity awareness training and sign acceptable use policies. Outsourcing your cybersecurity is also a benefit when shopping for cyber risk insurance policies.

In addition, read the fine print before signing on the dotted line. Some policies exclude coverage for accidental employee actions that result in a breach, leaving you on your own if an employee unintentionally causes the incident.

Others may limit the time frame for paying out damages. In the case of an advanced persistent threat, this limitation can cost you big time since the breach takes weeks or even months to uncover.

Some carriers dodge payment of a cyber risk claim by refusing to pay out for an untargeted attack. In other words, if your organization was part of a bigger malware scheme rather than targeted for an attack, they will not honor the claim.

Keep in mind that some exclusions are entirely at the discretion of the carrier. A state sponsored attack, for instance, may be considered an "act of war" and your claim will be denied.

Before you can qualify for a cyber risk policy, your organization will need to undergo a cyber health evaluation. Again, the best way to prepare for this is by outsourcing your cybersecurity to a third-party who will conduct a pre-application network risk assessment.

Elements of a Successful
Transition in a Remote Workforce

While businesses were initially forced into a sudden shift to remote work, the trend will be a permanent one for many businesses. Now that the panic has subsided, it's time to evaluate your remote workforce strategies.

A successful remote workforce will have seven elements: technology, connectivity, flexibility, social interaction, clearly defined goals, communication, automation, and the right balance of freedom and oversight.

Technology

Your employees' success will be highly dependent on the technologies your teams are using. It's more than just the latest greatest hardware; equipping them with responsive and intuitive software is a key factor in productivity, communication, and collaboration.

Without technology that meets the demands of a remote workforce, your employees will become increasingly less motivated and productivity will suffer.

It's possible to have too many tools, however, and this will also negatively affect your employees. While you may be aware of all the big applications your teams use, are you aware of all the smaller tools used individually? Your design team may be using programs you have never even heard of, while the HR department runs another set altogether.

You routinely inventory all the hardware your employees use, but now you will need to inventory all the software programs and applications as well. Remember that unnecessary applications drain your network, add security concerns, and will often duplicate other processes and frustrate your teams.

Connectivity and Collaboration

Sharing files, data, and ideas must take place quickly or momentum will be lost. In the office, your employees could drop files onto a co-worker's desk, walk into a manager's office to share an idea or a concern, or schedule an impromptu meeting to discuss a project.

Cloud technologies allow the exchange of ideas, files, and data in real-time, and virtual meetings can be scheduled at the touch of a button.

Flexibility

Flexibility is an important part of a successful workplace journey. This flexibility is important in two ways:

- Managers and employees must learn to shift priorities quickly while keeping the main goal in sight. Many employees have had to learn new skill sets to keep their teams rolling, and business leaders should always find opportunities for employees to expand their roles.

- Flexibility of scheduling is important part to an employee's sense of work-life balance. Remember that working from home means that kids may also be schooling remotely. Additionally, many services are limiting the number of employees they have in-house or the number of visitors they allow into a facility at a time, so your employees may need schedule shifts for things such as banking, doctor visits, and so forth.

Employees are more than willing to work earlier or later to make up for time missed due to obligations. Ask for employees to schedule their workday interruptions whenever possible and give them the freedom to make up the time by adjusting their work hours. In fact, employees spend more time working each day than they did in the office because they aren't up against a "hard stop" or a time-consuming commute.

Don't confuse flexibility with a lack of structure, though. Keep employees on point and on task through structured meetings and evaluations and make sure each employee "pulls their weight."

Social Interaction

Some employees may consider themselves introverts; they won't miss social interaction at all and can keep their own morale high while working remotely. Most of them, however, thrive on office interactions and will find themselves feeling isolated and depressed by remote work.

Encourage team building exercises and "extra-curricular" activities such as virtual happy hours, game nights, trivia, and book clubs. Teams can meet for virtual lunch breaks or early morning "breakfast" before the day begins. Some may enjoy just being "openly connected" during the workday.

Success for your remote workers will mean looking out for employees who are feeling isolated and encouraging interaction throughout the day.

Clearly Defined Goals

It's imperative to the success of your remote workforce that your teams' goals are clearly defined, priorities are tagged and recognized, and the tasks and projects needed to reach the goal are explained when they are assigned to the team.

Just because an employee is working from home doesn't mean s/he somehow has the time to work on three "high priority" projects at once, and not being clear with your remote workforce about expectations, due dates, and goals will leave them confused and overwhelmed.

Work backwards. Define the goals first, then establish its priority in "the grand scheme of things," and lastly assign the tasks to the most appropriate team members.

Communication

A successful workplace journey means open lines of communication between teams, managers, and individuals.

Remember that there is always more than one way to interpret a conversation. Everything from cultural background to age differences can muddy the communication lines. This means occasional crossed signals when it comes to completing tasks and projects. Encourage employees to reach out with anything that may seem unclear and keep your patience with employees who seem like they don't "get it" right away.

Keep the lines of communication open, starting with a brief daily team meeting in the morning to allow employees to discuss any confusion or unclear tasks with the group. Ineffective communication can mean "stepping on toes," duplicating work efforts, and projects that have veered wildly off-course.

Automation

A successful remote workforce will need automated processes to stay productive.

Automation can be used to create workflows in every aspect of your business, such as scheduling regular meetings, employee and client onboarding, recurring email and communications with clients, billing, and purchase orders.

IT automation can include systems tests, alerts, data transfer, backup and recovery data collection, and much more.

Automating processes frees employees from mundane tasks and reduces human error. The more you can streamline your processes and use automation, the more successful your remote employees' journeys will be.

The Right Balance Between Freedom and Oversight

It can be hard to strike the right balance between giving employees freedom and understanding how much management is necessary. At the end of the day, the employee's work will speak for itself. Some function best when given autonomy while others require a more structured work environment.

The problem is that swaying too far one way or the other will lead to lower employee motivation, lowered productivity, and increased employee dissatisfaction. No highly motivated self-starter wants to be micromanaged, but conversely some employees need a more detail-oriented management style when working remotely.

As a business leader, you have already identified each employee's unique "work style." This won't change just because they are now part of a remote workforce; your self-starters will remain self-starters and those who need more guidance will continue to need more guidance regardless of where they are working.

Don't be tempted to manage all employees the same way; use your weekly evaluations and progress reports to judge the level of management an employee needs to be successful.

The hardest thing a manager can do is to "let go," but a team built on respect and trust will yield far better results than a resentful one. Check in and checkup but try not to tip the balance between autonomy and accountability.

Embracing the Human Side
of the Remote Workforce

The times of sterile office environments are gone forever, replaced with personalized workspaces and views into an employee's lifestyle that were not possible before.

In days gone by, a barking dog or a cat walking across a camera view during a meeting would have been appalling. In today's work-from-anywhere landscape, however, these hiccups and occasional distractions are appealing. They are a welcomed chance to connect with each other on a far deeper, personal level than ever before.

While all remote employees should be encouraged to set up a home office in a quiet location, many of them weren't prepared for the shift and don't have the possibility of a dedicated "office" in their homes. They may share workspaces with children and spouses, too. For some employees, a "home office" could be a corner of the dining room, a kitchen table, or any unoccupied space where they can set up a workstation.

Zoom offers many downloadable options for backgrounds that block out unwelcomed "office scenery," but the overall experience of remote meetings may still involve unwelcomed distractions.

These distractions have been a unique way to deepen connections between coworkers as well as with clients, however. Dogs, kids, and décor have become a way of seeing the "human side" of each other, giving greater opportunities to share interests, strengthen bonds, build trust, and enable deeper conversations.

If these distractions aren't a constant occurrence with your employees and aren't disruptive to the flow and tone of a meeting, embrace the things that make your teams "human." The modern workplace journey has redefined acceptable meeting environments, allowing participants to relax and open the lines of communication in unprecedented ways. Remember that household activities cannot always be scheduled around meetings, and life will continue whether it's on camera or not.

If an employee's disruption is disturbing a meeting, however, encourage them to mute themselves and turn off the camera until they can turn their full attention back to the team. Set guidelines to minimize disruptions whenever possible, such as turning off phones and not checking emails or alerts while the meeting is in progress.

The New Role of Managed Services Provider
in the Remote Workforce Environment

Managed Services Providers are teams of professionals who work together to implement the best strategies for businesses, along with giving them help and support. MSPs are familiar with industry regulations and play a key role with compliancy agencies. An MSP brings knowledgeable professionals under one roof to address any IT issues that come up, help with planning and strategy, conduct training sessions, and monitor your network's health with event logs and routine testing.

The role of an MSP should be a proactive one, seeking to stop small issues from becoming big issues by preventing them altogether. The responsibilities of an MSP have grown in the modern workplace however, and MSPs are increasing their roles to meet the challenges of a remote workforce.

Auditing, Supplying and Tracking Equipment

Because MSPs tend to have relationships with equipment suppliers and vendors, businesses will find that the IT provider can equip remote employees for less money than the organization could. Most small to medium-sized businesses were not prepared to supply equipment for their employees, resulting in remote workers using their own unsecured equipment.

Now that the dust has cleared, businesses are making a point of trying to equip remote workers for the long-term. MSPs can provide this equipment as well as taking on the documentation associated with it, including tracking serial numbers and models to assure each piece is accounted for. The MSP will also be able to keep track of when a device was issued, and when it will need routine maintenance or an upgrade.

Regulatory Compliance Specialists

Regulations have not relaxed in the modern workplace; in fact, they are increasing to meet the vulnerabilities of sensitive data storage, collection, and transfer in a remote world. The only constant thing with regulatory agencies is that their requirements will change often, and often seemingly without warning. Along with the changes comes a deeper reach into businesses' processes, and steeper fines for violations.

MSPs have taken on the responsibility of changing procedures to meet regulatory demands. They have also taken on a role of champion, defending businesses who find themselves on the wrong side of regulations and bearing the responsibility of violations.

Technical Support

MSPs have taken on even more of a supportive role for their clients, expanding remote troubleshooting services and help desk service hours. Luckily, these trained professionals have a deep pool of talent that can usually fix IT issues in real-time, and often without a service call.

The alternative to ongoing technical support from an MSP is costly break-fix repairs, often done by random technicians who have no true understanding of your organization's infrastructure.

Strategists and Problem Solvers

Businesses have been forced to make major adjustments to their IT strategies when they first transitioned to a remote workforce and are now reassessing their approach so they can sustain their employees in a work-from-anywhere landscape.

MSPs have always been a valued resource for business planning and strategy. Now more than ever, businesses must turn to the professionals to create strategies and solutions that provide remote employees with the tools they need, and the increased security platforms businesses require in the face of elevated cyber threats.

Partnering with an MSP for business planning and strategies will also keep businesses' IT solutions on track and within budget. MSPs will help with overall business strategy planning as well as helping organizations plan for future IT projects such as upgrading hardware.

MSPs will not only provide the new roadmap businesses need to sustain their remote workforce, they will help implement the strategies, too.

Identify and Access Management

MSPs are managing identification and authorizations for remote workers. From assigning permissions to implementing multi-factor authentication, Identity and Access Management (IAM) strategies keep your employees connected to the files and applications they need to perform their job duties while restricting access to the applications and files they don't.

Devices have no way of identifying users and without robust IAM, hackers can gain access to devices and files by hacking a device. IAM limits the files a hacker can access, protecting your network and files and limiting the damage caused by a breach.

A robust IAM (Identity and Access Management) will help keep your business aligned with regulatory requirements by limiting access to sensitive data.

Choosing and Implementing the Right Tools, Software, and Applications

MSPs have the largest book of talent and resources to help each business choose the right tools for their remote workforce. MSPs can often supply these tools at a lower price because of partnerships with third-party vendors.

An MSP will look at your business' size, workload, goals, and industry requirements to align tools and applications to your unique needs.

Cloud services are one way to keep your remote employees connected, and an MSP will help you choose the right cloud solutions based for your company. They will also help you assess what applications and files should be cloud based, and which can remain on servers.

MSPs will take on the responsibility of moving your company to the cloud and supporting your cloud services.

How a Partnership with Integris
Will Help you Sustain your Remote Workplace

Integris is the perfect partner for small to medium-sized businesses at any stage of this journey into sustaining a remote workforce. When businesses were suddenly forced to adapt to remote work, Integris was prepared. Our clients were able to make the shift easily and will be able to sustain remote work indefinitely because we had already predicted the shift from office work to work-from-anywhere.

In fact, Integris had already embraced some work-from-anywhere positions within our own organization long before it became a necessity; we were already well-established with the tools, technologies, and strategies businesses needed to make the transition. Our forward-thinking proactive solutions kept (and continue to keep) our clients on top of the trends and technologies they need to thrive.

Our partners can use us to supplement their own IT departments with co-managed services, or choose to outsource their IT completely with our fully managed IT services.

Integris specializes in solutions that decrease unplanned downtime while increasing productivity, connectivity, and reliability. From our innovative cybersecurity platform, to our staffed Security Operations Center and dedicated tech teams, Integris puts your business first. We specialize in business planning and strategy, cloud migration and solutions, and responsive support and help desk services. We offer flexible packages that will fit any budget, and our services save businesses more money than relying on break-fix repairs or boxed solutions.

For more information about the next steps to sustain your remote workforce, reach out and speak with a friendly IntegrisIT professional today.

Contact us and schedule your FREE IT consulting session today!