TECHNOLOGY BEST PRACTICES FOR ENABLING REMOTE WORKERS

Business considerations, best practices and key questions to ensure a successful remote working program.

Remote working programs have well documented business benefits, but too often tech solutions and planning stand in the way of a truly streamlined and successful program.

Business managers and IT teams should discuss these best practices and key questions to create a program that runs like a well-oiled machine.

DIZZION

TECHNOLOGY BEST PRACTICES FOR ENABLING REMOTE WORKERS

Business considerations, best practices and key questions to ensure a successful remote working program.

As of 2017, 43% of US employees work remotely in some capacity, according to Gallup. The shift is largely driven by employee desire, with 57% of today's workers saying that working from any location, anytime is important to them and 37% admitting they'd switch jobs for the ability to work remote at least part time. Nearly every industry is feeling the effects of this workforce change and remote working is now being embraced by organizations from contact centers to highly regulated industries like finance and healthcare.

As this change in worker sentiment ticks higher, organizations have to find ways to accommodate employee wishes or risk losing top talent. Luckily, employees aren't the only ones that benefit from remote working programs.

The Business Case for Remote Worker

When properly implemented, organizations that allow for remote working can see a range of business-focused benefits, from cost savings to better access to talent.

- 49% of employees say the ability to work from any location, anytime has the greatest impact on how productive they are. (Source)
- Employees who spend 60%-80% of their time working remotely are the most engaged and feel they make more progress during the day than employees who work remote less. (Source)
- 95% of employers say telework has a high impact on employee retention. (Source)
- The average business can save up to $11,000 per employee annually by allowing for part time telecommuting, largely from real estate and utility savings. (Source)

While those benefits alone might be enough to encourage organizations to allow remote working, a policy change this big and impactful isn't as simple as sending everyone home to work.

Planning for Remote Working

Successful remote working programs require careful planning and follow through. Not only do management approaches change as teams become spread out, but IT support and user experience also become more challenging. Organizations evaluating remote working or work at home programs need to carefully consider how they'll enable the practice from a practical and technical perspective.

Key considerations include:

- How endpoint devices, peripherals, desktops and applications will be provisioned to remote users
- How data and desktops will be kept secure
- How remote workers will be monitored and supported
- How the program will be evaluated for success, optimization and enhancements

These considerations aren't only important to IT or the organization, they can also have a major impact on the end user experience and, ultimately, users productivity. A poorly planned, executed or supported remote working program can result in a drop in productivity, which will have a negative impact on the company and employee morale and will quickly sink the initiative.

Provisioning Desktops & Devices

One of the most basic elements of enabling remote workers is deciding what endpoint they'll use and how that endpoint will be provisioned. There are several approaches ranging from supplying full laptops to tablets to implementing a BYOD model. Each approach has unique benefits and challenges, and it ultimately comes down to an organization's preference.

No matter how organizations choose to provision devices, it's important that proper planning take place to ensure all remote users have the right applications and computing power for their specific use cases. Poorly planned or provisioned instances will result in a poor user experience and lead to frustration, depressed user engagement and degraded productivity.

42%

of organizations are actively deploying BYOD program.

Best Practices

Best Practice 1

Fully understand the total cost associated with whichever provisioning option you choose. The questionnaire below highlights key considerations, many of which will have associated financial costs that differ based on whether you choose to provide an endpoint or rely on BYOD.

This should include the life expectancy of the endpoints since some will require refreshing and replacing sooner than others (i.e. the useful life of a laptop can be extended when paired with virtual desktops).

Best Practice 2

Consider what peripherals will be required with each approach and create a documented list of approved peripherals to ensure compatibility.

Best Practice 3

Carefully define specific use cases, detailing which applications are required, how much computing power is needed, etc. before deciding on a solution.

Best Practice 4
Discuss the desired time requirement for provisioning a new employee. Having a benchmark of how long the task should take will help you measure potential solutions.

CASE STUDY

"Before Dizzion, the service desk would connect remotely with remote agents and install a virtual machine. Especially for agents with lower bandwidth and internet connections, it could takes 6-7 hours to download. We would eat the cost in productivity for that first install, but if the VM got corrupted, the agent would be down for an entire shift while we reinstalled a new virtual machine."

— Brent Hernandez, Transcom

Best Practice 5
Choose a consistent, standardized approach to hardware, endpoints and peripherals to minimize difficulty and future proof the program as technology needs evolve.

Best Practice 6
Have a plan to revoke access to corporate data and applications once an employee or contractor no longer works for the organization. (This plan should also include how you will regain possession of any company-issued devices.)

Questionnaire

- What applications are required per use case?
- What functions does the desktop need to support, per use case?
  Examples:
  - *Telephony integration*
  - *Softphone integration*
  - *Video conferencing & video chat*
  - *GPU-heavy applications*
- How much computing power (CPU, memory, etc.) is required per use case?
- Is application streaming an adequate replacement for a full desktop for select use cases?
- What endpoint with the remote employee use?
  Examples:
  1. *Company issued device provisioned by IT and shipped to the employee*
  2. *Employee's personal device (BYOD)*
  3. *Thin client*
  4. *Zero client*

- What peripherals are required to accompany the selected endpoint?
  Example: Mouse, keyboard, monitor, headset, etc.
- Who will be responsible for providing the required peripherals (the end user or the company)?
- Is the chosen endpoint compatible with the required applications and software?
- How will the desktop be initially provisioned (loaded with the appropriate applications and security measures)?
  Example: If relying on BYOD will IT remotely log onto the employee's device? Will the employee have to download a virtual desktop client?
- How long is the anticipated or acceptable provisioning timeframe?
- If providing endpoints, have you budgeted for shipping costs and accounted for increased time to productivity?
- What is the expected timeline for revoking access after an employee/contractor no longer works for the organization?
- What is the expected life of the endpoint devices before a refresh will be required?
- What is the plan and timeline for replacing endpoints at needed?

The average cost of supplying a remote employee with a company-issued laptop is

$1,448

Securing Endpoints & Data

Whether you provide an endpoint or adopt a BOYD approach, you are still ultimately responsible for data security – particularly in highly regulated industries that must meet strict data protection and compliance standards. Maintaining data and endpoint security can be challenging when employees are not centrally located and IT must provide support remotely.

Best Practices

Best Practice 1
Remember that employees could be working from home, from coffee shops, from co-working spaces, etc. Because of this remote situation, your security controls need to be even stricter than in a traditional office setting and extend down through the endpoint.

Best Practice 2
Understand the challenges of ensuring security in a BYOD environment.

Best Practice 3
Understand the security capabilities of any endpoint devices you supply.

Best Practice 4
Identify specific security and control requirements based on use case, work being performed or user group.

Best Practice 5
Regularly review and update security practices and protocols and roll out any changes to all remote employees quickly.

Questionnaire

- Are controls and security parameters well documented based on user group or use case?
- How will you roll out updated security controls or changes?
- Is dual factor or multi factor authentication in place?
- Will vulnerability scans be run on the endpoint?
- Can information be saved in a vulnerable manner (i.e. to an local desktop or external drive)?
- Do security practices meet compliance standards (such as PCI DSS or HIPAA HITECH)?
- How will you ensure employees do not use the device for personal uses in way that may put corporate data/network at risk?
- Is data backed up for disaster recovery?
- Can the desktop be remotely wiped if the device is lost or stolen?
- If BYOD, how will you isolate corporate data and apps from the employee's personal uses?

Monitoring & Support

Every device requires ongoing support and maintenance to ensure it stays secure and in good operating condition. This can become challenging for remote devices if organizations don't have the proper practices and solutions in place. While it's easy to neglect devices that aren't in sight, leaving support and maintenance to remote workers leaves organizations open to major risk.

Best Practices

Best Practice 1
Create a documented maintenance plan and time table to ensure no endpoint goes unaddressed.

Best Practice 2
Adopt a solution that makes it easy for IT to remotely support, troubleshoot and update devices in a timely manner.

Best Practice 3
Don't rely on end users to be able to adequately explain the issues they're experiencing. Capabilities like remote sessions and real time monitoring are key to troubleshooting remote devices.

Questionnaire

- Who is responsible for repairing the remote endpoint?
- How will IT troubleshoot the remote device?
- How will you patch the device?
- How quickly will critical patches be applied to remote desktops?
- How will you update applications and software?
- How will the employee remain productive if the endpoint needs repairing or replacement?
- Is IT responsible for troubleshooting and/or replacing peripherals?
- How will you document, maintain and control application licenses?
- How will you monitor resource, application and license usage?
- How often will the "acceptable peripherals" list be updated?
- How will you track employee active versus idle time?

THE COST OF NOT PATCHING

The WannaCry ransomware attack in 2017 made headlines for the extent of its reach. But the damage could have been greatly mitigated if more organizations and individuals followed recommended security updates.

"Two months [before the attack], Microsoft released the patch that could have prevented the outbreak. But because so many companies didn't apply it, the so-called WannaCry attack spread like cholera." – NPR

Insights

The ultimate key to sustaining an efficient and effective remote working program is to not assume that all is well. On-going evaluation and deep insights are critical to optimizing the program and ensuring it's running as expected. Historical evaluation and trend analysis are particularly important in remote working programs since so many additional factors (such as location-based bandwidth) can have an unanticipated effect.

Having the right technology solutions in place to provide insights into remote workers' environments is important to bridge the management and support gaps created by remote programs. Key technologies allow management to gain insight into everything from remote worker productivity and effectiveness to logon logs and active/idle time. Without this information, organizations cannot accurately judge the effectiveness of remote working programs.

Best Practices

Best Practice 1
Establish remote-specific KPIs for both remote workers and for the staff supporting remote programs.

Best Practice 2
Regularly revisit the success and challenges of providing tech support to remote workers and address any outstanding issues to make the program more effective.

Best Practice 3
Regularly review resource and license usage to make sure spending and performance are optimized.

Best Practice 4
Poll remote workers and their managers to see what aspects of the program need improving.

Questionnaire

- How will you track, measure and report on KPIs?
- Are remote employees equally, more or less productive than in-house employees?
- Is active vs. idle time within the organization's expectations and threshold?
- Are logon times across remote workers within the organization's expectations and threshold?
- Do you have unused software licenses?
- Is a user group continually struggling with IT issues?
- Is IT able to meet the established provisioning and support timelines?
- Have an unanticipated security issues arisen stemming from remote working programs?
- What is the average cost to support a remote employee (i.e. provisioning devices)?
- What are the estimated cost savings of allowing employees to work remotely?

WHAT TO READ NEXT

ABOUT DIZZION

Established in 2011, Dizzion is a global provider of end-user computing services, including cloud-delivered Desktops as a Service (DaaS), paired with complementary offerings like secure endpoints, application delivery and storage. The company is delivering the next generation of virtual desktop solutions to meet the demands of a remote global workforce in industries with stringent security and compliance needs, including business process outsourcing, financial services, healthcare and insurance. Dizzion's mission is to enable users to securely access applications and data from any device, anywhere increasing mobility and productivity. To learn more about Dizzion, visit **www.dizzion.com**.

SEE HOW DIZZION CAN HELP YOUR REMOTE WORKING PROGRAM

REQUEST DEMO ⟶