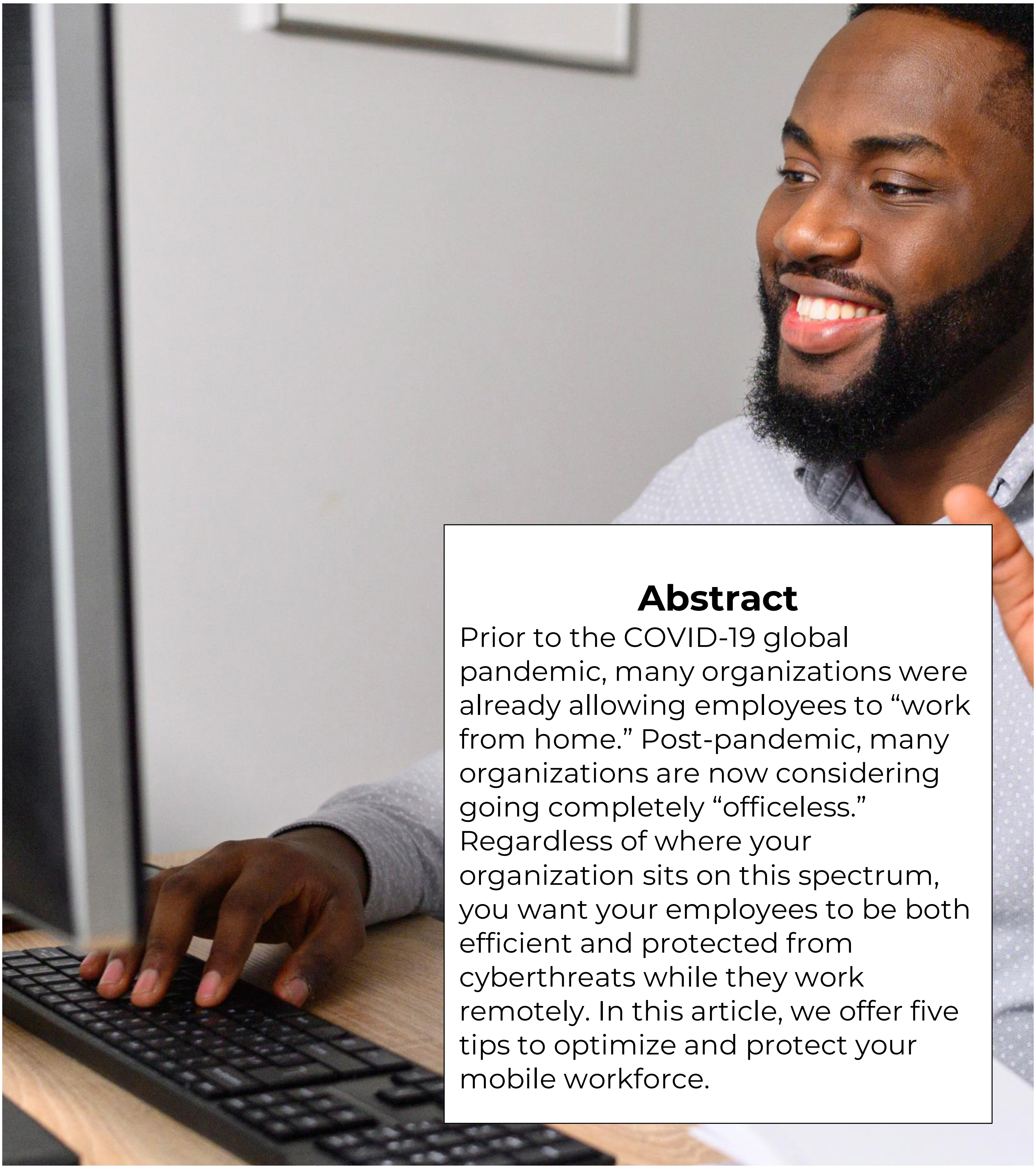
Top 5 Things to Protect and Improve the Productivity of Your Remote Workforce

Danny Cota
Co-Founder, GSDSolutions LLC

A seasoned technology professional, Danny Cota currently runs **GSDSolutions**, a Managed Services Provider, with his Co-Founder, Scott Davison.

GSDSolutions provides subscription-based IT services for small and medium sized businesses and non-profits.



Abstract

Prior to the COVID-19 global pandemic, many organizations were already allowing employees to “work from home.” Post-pandemic, many organizations are now considering going completely “officeless.” Regardless of where your organization sits on this spectrum, you want your employees to be both efficient and protected from cyberthreats while they work remotely. In this article, we offer five tips to optimize and protect your mobile workforce.

Introduction

The five tips in this article will consist of three tips on how to improve your mobile workforce's collaboration and communication internally. Some of these technologies can be leveraged outside of your organization as well. Two of the tips we mention are really the bare minimum of cyberthreat risk mitigation that you should be doing for your remote workers.

Lastly, a "top five" list of this kind can in no way be comprehensive. Our goal here is get you up to speed on the most critical areas required to help your mobile workforce succeed.

Assumptions:

- This article will not endorse one Operation System (OS) platform over another – we happen to like both Windows and the MacOS.
- We will not endorse any particular hardware vendors other than to say that Dell, HP, Microsoft, Lenovo and Apple all build good, reliable laptops at price points that can accommodate just about any budget.
- We assume that whatever laptop hardware that you've supplied to your employees has enough processing power (CPU and RAM) and storage space (choose SSDs over HDDs) for them to run their important business applications properly.

Implement a robust infrastructure to ensure optimum productivity for your mobile workforce.

Ditch the "File Server!" (Cloud Storage and Sync)

- Technical difficulty to implement: **MEDIUM**
- Typical cost: **FREE to $100+/user/month.** (Prices vary widely depending on desired features, storage required, users, etc.)
- Typical "bells and whistles" for an additional fee:
  - Unlimited storage and/or file version retention (borderline backup)
  - Legal hold functionality
  - SAML (Security Assertion Markup Language) integration
  - Multi-user administration
  - Regulatory compliance (HIPAA, etc.)
  - Data Loss Prevention (DLP)
- Vendors of note:
  - Microsoft, Google, Egnyte, Box, Dropbox, Citrix (Sharefile), etc.

The traditional "file server" is slowly but inexorably going the way of the dodo. If your organization is still using in-office file servers and VPNs to connect to that data, consider migrating most or, ideally, ALL of that data to a cloud-based storage solution. These solutions maintain the security of your data while still allowing your workforce to access that data from anywhere on the planet with relative ease.

Cloud-based file storage and sync tools are the first step in optimizing your mobile workforce.

Pick a Single Web Conferencing Tool

- Technical difficulty to implement: **LOW**
- Typical cost: **FREE to $20/user/month.** (Again, prices vary depending on vendor, features, number of users, etc.)
- Typical "bells and whistles" for an additional fee:
  - Increased number of allowed meeting attendees
  - Corporate branding
  - Storage for meeting recordings
- Vendors of note:
  - ZOOM, WebEx, GoToMeeting, Microsoft, Google, etc.

There are lots of good web conferencing platforms on the market today. Contrary to popular belief, ZOOM has not eliminated all of its competition yet despite the COVID-19 pandemic.

The suggestion here is not that you should use only one web conferencing platform--you cannot always control what platform people outside of your organization will use. Rather, the suggestion is that **internally** you choose a single web conferencing platform so that you can consolidate training on that tool. Doing this can also help you reduce the cost per user, as tool vendors will often offer greater discounts when more users sign up.

Pick one web conferencing tool for your team to consolidate training and save money!

Use a Chat Tool

- Technical difficulty to implement: **LOW**
- Typical cost: **FREE to $15/user/month**
- Typical "bells and whistles" for an additional fee:
    - Unlimited message storage
    - SAML integration
    - DLP and legal hold/discovery
    - Regulatory compliance
- Vendors of note:
    - Slack, Microsoft Teams, Asana, Basecamp, etc.

While traditional email is not going away anytime soon, it's not the optimal communication and collaboration platform that we would like it to be. Sending attachments back and forth among multiple recipients can be cumbersome and time consuming.

Modern chat/collaboration tools make it easier to share files, graphics, ideas and other data with relative ease. Conversations on these platforms are easily searched, and administration of these tools can also be distributed to members of your team as you see fit as well. (Think: Marketing team channel, Engineering team channel, etc.)

A great chat tool is the third leg that forms the stool (along with the other two tools previously mentioned) on which your organization rests its collaborative powers on!

A good chat platform greases the "wheels of communication" and collaboration for your team.

Antivirus Software

(Often, also referred to as “antimalware software” or “endpoint protection.”)

- Technical difficulty to implement: **LOW**
- Typical cost: **$3 to $5/month.** (Usually includes protection for 1 - 5 computers.)
- Typical “bells and whistles” for an additional fee:
  - Data backup solution (usually cloud-based)
  - Password management software
  - “Dark Web” monitoring
  - Secure VPN solution
  - Cybersecurity insurance (covering up to some dollar amount in losses incurred by a data breach)
- Vendors of note:
  - Symantec, Webroot, Cylance, SentinelOne, Carbon Black, etc.

For just a few dollars a month, antivirus software delivers the most “bang for your buck” in terms of managing various data security threats, including ransomware. It should be your minimal “first line of defense” for your mobile workforce.

Antivirus software is inexpensive and a MUST HAVE for all of your organization’s computers!

Backup Your Data Regularly

- Technical difficulty to implement: **LOW**
- Typical cost: **$3 to $10/computer/month**
- Typical "bells and whistles" for an additional fee:
  - Local backup (in addition to cloud-based) storage
  - Multiple computer backup
- Vendors of note: Backblaze, Carbonite, Crashplan, Acronis, IDrive, etc.

If you have a computer and you have data on it that you care about, then backing up that data is simply a MUST DO. Should a specific laptop's hardware fail, or should the laptop's user fall victim to cyberthreats like ransomware, then restoring your data from backup is going to be your quickest path back to productivity.

Note: It is important to understand the difference between **backup** and **file-syncing** tools. File syncing tools, e.g., Dropbox, Google Drive, Box, etc., are NOT backup tools! Rather, they are file *replication* tools. File *backup*, on the other hand, maintains a discrete history of your backup files, allowing you to restore files from previous points in time.

Backup your data. Period.

Final Thoughts

As noted previously, this article is meant to cover the basic elements of providing an optimized and safe remote work experience for members of your team. More "advanced" topics in this area might include:

- Mobile Device Management (MDM) to ensure that all corporate laptops are encrypted and can be remotely wiped in the event of loss/theft;
- Maintaining a supply of spare laptops that can quickly be shipped to employees who have laptops that have recently failed;
- "Cloud VPN" solutions are also becoming a popular way to ensure that only the people who should have access to organizational data have access to it as well.

Keep in mind the following points:

- The risks and challenges associated with a mobile workforce, e.g., collaboration and cybersecurity, are relatively inexpensive to address via technology.
- From a technical perspective, the solutions that we've discussed are also relatively simple to implement.

Notice that we say here "simple" instead of "easy" because the later implies "not difficult", while the former implies "not complicated." Some of these solutions, for example, may be difficult to manage for a large team using a relatively simple solution.

Providing your employees with a good remote work experience is relatively inexpensive and simple to do.

Still Have Questions? We’re Here to Help!

Should you have any questions about the technologies discussed here (or any other technology-related questions), please email us at **getstuffdone@gsdsolutions.io** or call us at **(650) 282-7695**.

About GSDSolutions

Simply put, GSDSolutions is a customer service company. True, our particular flavor of customer service happens to center around technology – computers, software, cybersecurity, etc. – but, ultimately, our job is to serve our customers. We serve our customers in the same way that we would want to receive services ourselves – that is, with integrity, with wisdom and a dash of empathy thrown in for good measure.

https://gsdsolutions.io/