We're Going to Get You Out of the Technology Rut

Is the technology your business relies upon composed of bits and pieces of tech you've incorporated gradually over the years? While all of your computers and devices may work, are they actually working for you? Your investment into IT was supposed to make your staff more productive—is it, or has it plateaued?
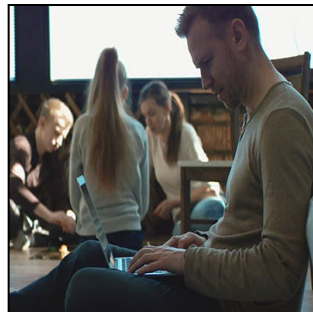
Is Your Business' Technology Still Working For You?

That's the million-dollar question...

Read the Rest Online!
https://dti.io/technologyrut

YEARS IN BUSINESS
est. 1993

Employing Remote Workers Carries New IT Challenges

Remote work carries with it a different set of risks than does a traditional workplace setup. Being forced to move in that direction only exacerbates the issue of figuring out how to operate under what people are calling the "new normal". This month we thought we would go through a couple of the risks that come with having your staff working remotely, and what to do about them.

Before we get into it, we just wanted to recognize that not all remote workforces are due to the lingering global pandemic. A lot of businesses needed to provide computing support for employees who work out of the office due to travel and other factors. Many times, employees have to go to the customer to bring value and having a business that can properly mitigate the risks can mean better situations for those paying for the product or service.

Risk #1 - Lack of Focus Among Remote Employees

For the business that was against allowing remote work and forced to change their business strategy because of COVID-19, having employees that are just not as focused as they were when they were working in an office is probably one problem you've encountered. According to a Harvard Business Review study, many workers are feeling disconnected from their co-workers; a real costly problem if your business directly depends on collaboration or their ability to collaborate with your other staff members.

Studies suggest that over time remote workers improve their collaborative productivity, but can you afford to see your productivity drop at a time when there are so many demands on your business? You can if your business has dedicated and experienced workers that know what is expected of them and deliver on deadlines. If your business is working

Yes, Your Business Can Use Outsourced IT Services!

Finding talent can be difficult for businesses, especially for those that are challenged by variables such as their geographic location (not as big of a problem thanks to remote employment), but more often than not, budget will be the key holdup for small businesses seeking top talent. Thankfully, even small businesses can hire top talent through the process known as outsourcing, which is particularly helpful for acquiring talented and qualified IT professionals.

What is Outsourcing?

Outsourcing is when a company hires an external organization or business to take care of specific processes or tasks that cannot be done by the company itself. IT is a common way that outsourcing is used because of the immense amount of technical knowledge and expertise required in order to be an effective technician or resource. Whether or not outsourcing IT is the right call for your organization will depend on your current amount of knowledge and resources in this field, but no matter where you fall on this spectrum, outsourcing IT can be a helpful strategy.

Some folks believe that outsourcing is essentially admitting that your organization can't handle tasks on its own and is, therefore, reliant on others to be successful. On the surface

directive

"Mistakes are a fact of life. It is the response to the errors that counts."
- Nikki Giovanni

PAGE 2

Why Multi-Factor Authentication is the New Complex Password

Everyone always tries to drive home the importance of passwords, but the simple fact of the matter is that passwords in today's day and age are not enough to keep your business safe. While passwords are still important, they play a relatively small role compared to some of the more advanced security features that businesses must implement in order to stay as secure as possible.

One of the best ways you can keep your company safe is by implementing multi-factor authentication. This strategy entails exactly what it sounds like it does: multiple factors that all contribute to account security. While passwords will still be necessary, additional factors will also be required, such as biometrics or secondary devices and accounts. The ideal way to take advantage of multi-factor authentication is to have at least two of the following:

- Something the user *knows*
- Something the user *has*

- Something the user *is*

You can see how each aspect of authentication factors in here; something the user knows is a password, something the user has might be an external device, and something the user is might include biometrics like face capture, fingerprinting, or retina scanning.

As for why multi-factor authentication is important, consider what happens if a hacker steals your password and you do not have multi-factor authentication enabled. They have access to your account, and all it took was a simple copy and paste of your password. Now imagine what would happen if a hacker were to find your password if you have MFA activated. They would be prompted to enter the password, but without your smartphone to receive the passcode or the literal eyes in their sockets, they will be out of luck.

At the end of the day, the more steps you put between your account access and a hacker, the better. Simply put, the majority of hackers are lazy. They want to pick the low-hanging fruit, as it is most likely to achieve a return on the time investment compared to spending hours and hours cracking one singular

password. It makes sense for them to move on to another lucrative prospect than waste time trying to crack the code.

Therefore, you want to take your organization's cybersecurity as seriously as possible, authentication included. Instead of leaving yourself as low-hanging fruit for hackers to pick at their leisure, place yourselves at the very top of the tree with powerful security solutions designed to make things as difficult as possible for hackers. They might move on to less-protected victims, but hey, at least it's not your business, right?

Directive can equip your business with the cybersecurity tools it needs to keep operations in peak condition. We can help you implement everything from unified threat protection to password management to multi-factor authentication, and it's so hands-off on your part that you won't believe how easy and streamlined the process is. To learn more about what we can do for your business, reach out to us at 607.433.2200.

Share this Article!
https://dti.io/multifactor

Employing Remote Workers Carries New IT Challenges

with inexperienced workers or new hires, having them work remotely may be problematic as there is an inherent lack of oversight.

> **...a couple of the risks that come with having your staff working remotely...**

The best way to ensure that your employees maintain focus is to promote dialogue about their jobs. This means clearly define your expectations and talk to them about stressors that may cause distress. For the worker that is not used to working from home, the shift to remote work may actually be detrimental to their mental health, and therefore will not help their work performance.

Risk #2 - Lack of Tools Needed to Accomplish Expected Goals
Another risk that should be pretty obvious is a workforce that lacks the tools to do the jobs they are expected to do. This could be as simple as getting them a workstation that allows them to efficiently do their tasks, or it could be an end-to-end issue that includes collaboration and communications tools. The remote workforce has different demands than does a staff that works in-house, so understanding that you may need to alter your strategies is a good first step in getting your staff the tools they need to succeed.

For the average remote worker, there will be a set of technologies that you will need access to, not to mention the

access they will also need to the data and applications that allows them to directly complete their workloads. Some of these tools include:

- Video conferencing
- Productivity suites
- Remote desktop/virtual private networks
- Project management tools
- Communications (email, instant messaging, VoIP, collaboration tools)
- Cloud storage
- Business management tools...

Read the Rest Online!
https://dti.io/tryremote

Yes, Your Business Can Use Outsourced IT Services!

(Continued from page 1)
this might appear true, but whether you realize it or not, your organization is always relying on others, even if it is hiring other employees. You'd rather hire someone who knows what they are doing than rely on others who don't know what they are doing, and with processes as intensive as IT, you don't want to leave any room for error.

How Can Outsourced IT Be Helpful?
Outsourcing IT services is one example of how outsourcing can help companies, but there are many different ways that you can utilize outsourced IT for your company. Due to the complexity of IT services in general, there are plenty of opportunities to improve operations through the use of it.

Here are four benefits that your company can take advantage of through the use of outsourcing your IT management to a third party.

- **Consistency with talent:** Access to talent can vary by geographic location, but with outsourced IT, you are not as limited.
- **Efficiency with access:** Outsourced IT services can mostly be performed remotely without an on-site visit, allowing for more accessibility and flexibility.
- **Affordability with budgeting:** Most outsourced IT services follow the "as a service" model in which you pay on a monthly basis for services rendered. This makes outsourced services easier to factor into a budget.
- **Flexibility with delegation:** If you

have in-house IT resources, outsourcing certain tasks to a managed service provider gives you flexibility in regards to how you utilize your existing resources.

Get Started with Outsourced IT Today
If you would like some guidance in making the decision about outsourcing your IT resources, Directive is happy to help facilitate that discussion. Even if you do have current IT resources, you can still find value in outsourcing certain aspects of your technology management to a third party like Directive. To find out how you can start reaping the benefits of outsourcing IT, contact us today at 607.433.2200.

Share this Article!
https://dti.io/3rdparty

3 Reasons Why Your Business Should Utilize Automated Cloud Backups
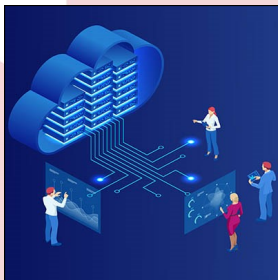
Data backup is something that some organizations think they can do without, simply because they believe that it's only valuable to have in the event that something wrong happens. Well, we're here to break the bad news that if something can go wrong, it most likely will go wrong… at least at some point. With automated cloud backups, however, the chances of some unexpected emergency ending your business are drastically reduced.

We'll give you three good reasons to utilize an automated cloud backup system; we think you'll find them too good to pass up.

Complete Redundancy
One of the biggest benefits of cloud-based backup comes from the fact that redundancy is a priority. You may have heard of the 3-2-1 rule, but we'll give you a refresher just in case. The idea is that you have three backups of your

data total: one stored on-site for ease of recovery and two stored in secure remote locations, one of which is located in the cloud for, again, ease of recovery. With this kind of redundancy, it's easy to see why automated cloud-based backups are such a valuable asset for any future-minded business.

Minimal Downtime
The entire purpose of a data backup is to be deployable in the event of a disaster, and when one of these hits your business, time is of the essence. You can't afford to wait around for a tape backup to get delivered and painstakingly restored while your office gets back into proper working order, if it can be done at all. Cloud-based data backups can be deployed at a moment's notice with minimal downtime, allowing your organization to maintain a specified level of operations until everything else gets situated.

Less Uncertainty
One of the biggest issues with…

Read the Rest Online!
https://dti.io/autobackup

Marketing Ideas & Tips for Your SMB

Write it Right: Sending the Message You Want With Your Content

Your content can serve a variety of purposes. It, of course, pulls traffic to your site and provides value to your visitors, giving them a reason to return and bringing you closer to a contact point. However, content can, and unavoidably will, also give your readership an impression of the "personality" of your company, through a variety of aspects. Of course, as a reasonable person, you want your website to describe your business in a way to make as favorable of an impression as possible on those readers who very well could become customers in the near future. Yet this is just the tip of the iceberg. If you wish to get a complete examination of what message you are sending to your readership, here are some steps you need to follow.

First of all, you need to evaluate the "voice" in which your content and advertising are written.

Is it cohesive? Does it sound like one person is writing it, or a dozen different authors are contributing entries to it? As your business' representative, the content and marketing materials that are distributed need to be read as though they are from the mouth of a single speaker - hence the term "voice." Fortunately, this is relatively simple to fix, if initially time-consuming. By establishing some language guidelines and compiling a style guide for your written content to follow, you can ensure that any content produced will share similar enough qualities that it appears to come from a single writer. This will reduce the discrepancies in separate pieces of content, and allow for your content to be recognizable by its tone.

Second (and really, throughout the entire process), it is critical to any message your content is trying to send that you proofread.

Nothing destroys credibility faster than a misspelled word, and typos are far too easy to miss. After all, spell check isn't infallible, and not all programs for word processing feature spell check capabilities at all. Proofread everything before posting, Proofread it, have someone else proofread it, work on something else before going back and proofreading it again. If you cna find a quiet enough spot, proofread it out loud. It is imperative that you proofread.

See how that works? That single typo invalidated that entire paragraph, maybe even this entire article, didn't it? All it takes is a few switched letters to ruin your credibility and make your company appear careless and sloppy. The takeaway here: always proofread your content.

Thirdly, your content should be written from a place of authority.

While it might not be obvious at first, a reader will gradually lose faith in the accuracy and/or usefulness of your content if it is filled with phrases that imply uncertainty. Is your content filled with "maybe," "perhaps," and other such terms, while lacking concrete statements and solutions? If so, it needs to be revisited and heavily edited, and here's why: if the content is phrased in that way, all it will do is repeat what has already gone through the reader's head before they sought out an answer. If someone looks to your content for a solution and finds only what they had already come up with themselves with little to no value add, they will not likely return again if they need further help. Why would they? If your content isn't written with confidence, there's no reason a reader should...

Read the Rest Online!
https://dti.io/rightcontent
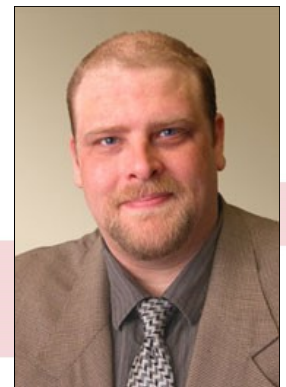
Chris Chase
CEO

Charlotte Chase
COO

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com

facebook.directive.com

linkedin.directive.com

twitter.directive.com

blog.directive.com

instagram.directive.com

NOW ASK THE SPIRITS IF THEY CAN TELL ME MY YAHOO PASSWORD.