TECH TIPS
TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

September 2021

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

How Co-Managed IT Could Save Your Company From Financial Disaster

When you consider the investments in your business that you can make as a CEO, you probably think to yourself, "Which investments will give my company the best ROI?" With that in mind, would you think of making a significant investment in bolstering your IT department?

Many CEOs are understandably hesitant to throw a lot of money into their IT department because the ROI is more difficult to estimate. That said, though, consistently updating your company's IT services is becoming increasingly crucial to the continued success, and indeed safety, of your company. Ransomware and other cyber-attacks that steal company data are becoming more frequent and more costly, while IT departments continually get the short end of the budgetary stick.

While that all undoubtedly sounds horrible, you might be wondering just what you can do about it. After all, you only have so much money you can invest back into your company's IT department, and it might not be sufficient for keeping your IT staff from getting burned out, disgruntled or making costly mistakes – even when they're performing their responsibilities to the best of their abilities.

What if there were a way that you could have access to the most up-to-date IT knowledge and software while also not having to shell out the funds necessary to update your systems and hire more knowledgeable employees? Well, that's where co-managed IT can be your company's life preserver.

Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks as well as assisting in your daily operations where needed. Think of it as "filling in the gaps" that your current IT department (try as they might) struggle to fill.

Continued on pg.2

Continued from pg.1

For instance, say your current IT department is great at taking care of the day-to-day fires that inevitably come up in a normal workday, but they struggle to get to the "important but not urgent" task of updating your company's cyber security and creating data backups. Maybe it's the other way around, where your IT department is very focused on security, but they struggle to find time to assist employees with password resets and buggy programs. Maybe neither of these cases describes your IT department, but they still need better access to the tools and software that would allow them to reach their full potential in protecting the company's sensitive information. Or maybe your company is going through a period of rapid expansion, and you just don't have time to build the kind of IT infrastructure that would best serve your needs.

Regardless of what your IT department's current needs are, co-managed IT is the solution. We're here to do the tasks and provide the tools that your current IT department just can't provide. Make no mistake, however: our intent is not to replace your current IT leader or team. In fact, we rely on the expertise that your IT department has about your systems. That's what makes up the "co" in "co-managed IT."

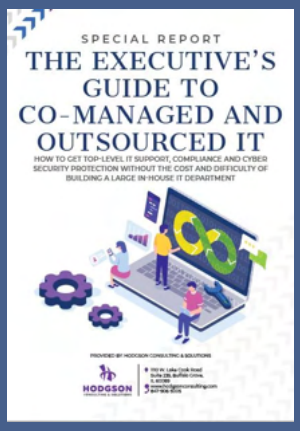
"Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks, as well as assisting in your daily operations where needed."

In order for co-managed IT to work, your company's IT department will need to see us as an ally in doing their job, not as an adversary. At the same time, they'll also need to be open to new ways of doing things. The world of cyber security is constantly changing, and if your IT department is set in their ways and unwilling to budge, your company will be left with an antiquated system, chock-full of valuable data that hackers and cybercriminals can easily exploit.

Finally, however, in order for co-managed IT to work, your company still must be willing to invest in its IT department. We know that the ROI might not be as clear as it is for some other investments, but trust us, the consequences of not having up-to-date IT services if (or when) hackers steal your sensitive data could financially devastate your company – or even end it altogether.

So, with that in mind, we hope you'll consider the benefits of co-managed IT and how it can make your company safe from cyber-attacks and bring you peace of mind.

Free Report Download: The Executive's Guide To Co-Managed And Outsourced IT



This eBook will give you important information on how to get top-level IT support, compliance and cyber security protection without the cost and difficulty of building a large in-house IT department.

Download your FREE copy today at
www.hodgsonconsulting.com/co-managed-guide/
or call our office at (847) 906-5005

Are You Protecting The Right Data?

You're ready to purchase a BDR. You've done all of the research, found a company you're confident in and are excited to finally have peace of mind. Now, you start thinking about exactly what you need to back up. Is all of your data necessary or should you salvage a little server room? Most businesses want to back up everything - you never know when you'll need it, but sometimes that is cost prohibitive

Depending on what kind of BDR you've purchased, you will first need to delegate what data is stored, is not stored, and how often. There are three different kinds of backup in today's tech world: straight to cloud services, software-based products, and a hybrid approach that combines on-site hardware and software with the cloud. The amount of data you can back up, how you can segment that data, how often it's backed up, how it's backed up (all the data every time creating enormous backups, versus incremental backups that key-in on changes) and how easy it is to access will be affected based on the solution you chose. It's not always necessary to back up everything daily, but there are some things you will want to consider.

First is credit card transactions or receipts. Your accounting software should keep an eye on this and automatically back up this data. This also includes things like invoicing, receivables, payroll and just about anything that is financially related. All financials are incredibly important, even one lost invoice could really hurt your business.

Second, protect all intellectual property. Unless you're rocking an amazing vault to store a famous recipe like Coca-Cola or KFC, make sure that you back up everything that brings you a competitive advantage in the marketplace. Anything with hackable data or items that could be compromised need to be backed up daily as well.

Next, you will want to back up any client files. Not only is it invaluable to keep this information safe, but it would certainly affect your client confidence if anything was lost or stolen. In addition to client files, make sure you're backing up your client and prospect lists (anything that you're storing in your CRM, really). You spend a great deal of time developing your list for marketing purposes. Losing this information is one of the major reasons companies go out of business within six months of experiencing data loss.

Finally, you must back up all project management software. Anything that your business uses to keep track of daily activities and work being done needs back up to make sure that you can maintain progress in the event of a data loss and you maintain a "paper trail" on project communication.

When it comes to BDR, you ideally want to back up every piece of data that you have. Sometimes, though, this is impossible based on the cost involved in maintaining that hefty data chain. At the bare minimum, keep these items in mind and you should never have to deal with a business killing disaster.

Authorities Seize Largest Stolen-Login Marketplace Site On The Dark Web

Earlier this year, the Department of Justice announced that they, along with other international authorities, had seized Slilpp, the largest site for stolen login credentials on the Dark Web. The site had over 80 million user credentials lifted from 1,400 service providers.

Authorities from four different countries all helped the FBI seize servers that hosted Slilpp. They also arrested and/or charged 12 people involved with operating the site.

Eighty million user credentials from 1,400 sites is a lot of sensitive information. That said, though, the Department of Justice still hasn't ascertained the full impact of the illegal activity on Slilpp. In the U.S., activity on the site led to almost $200 million in losses – and that's just a tiny fraction of the total activity.

The fight isn't over, but this case is a big win against illegal login sale marketplaces. The Department of Justice hopes for more seizures like this one in the future.

The Best Tips For Training New Hires

The hiring process is stressful. You

put in a considerable amount of work training someone for their role and hope they'll become a responsible employee. As difficult as this process is, however, you can streamline it with these tips.

Create A Scalable Guide For New Hires To Follow

Document all the responsibilities of the role and put them together in a concrete guide for new hires. This documentation will work especially well for visual learners, for recent graduates who are used to learning through guides and for non-native English speakers. In truth, though, anyone can benefit from having a set of principles to refer to.

Draw Examples From Real Life

When training someone in what to do in a specific situation, provide actual examples of what you did in that particular situation in the past. New hires will have an easier time completing their work if they have a previous example that shows them what to do.

Develop Your Interview Skills

Like great teachers, great leaders ask great questions to surmise if new hires are understanding their role. This will ensure that nothing gets lost in translation throughout the onboarding process.