Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: **Connectability**

CONSUMER CHOICE AWARD 2020 GTA — 3 YEAR WINNER

September 2021

This monthly publication provided courtesy of Ted Shafran, President of Connectability

---

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.
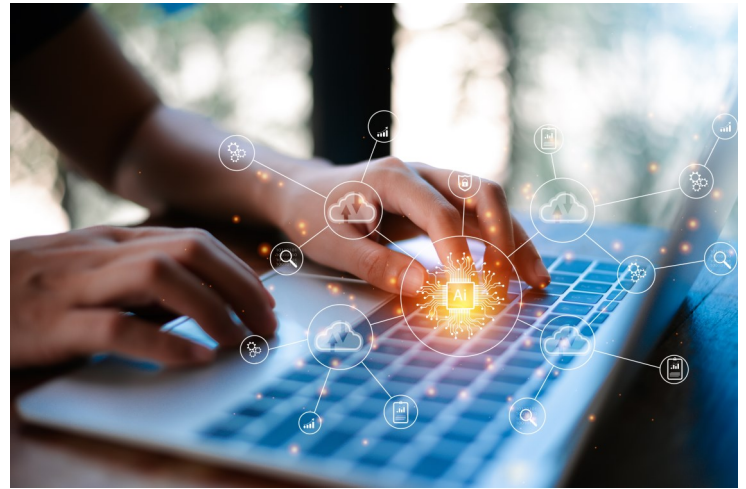
For instance, say your current IT

---

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. 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."

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

> **"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."**

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 change, 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 must still 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.

Exclusive FREE Report:
21 Revealing Questions You Should Ask Any Computer Consultant Before Giving Them Access To Your Computer Network

Choosing the wrong computer consultant to support your network can not only be incredibly frustrating and expensive, but could end up costing you in downtime, data loss, and expensive repair bills, not to mention the headaches and frustration!

Even if you aren't ready to make a change right now, this report will give you important questions you should ask your current IT person to make sure their policies, procedures and service standards won't leave you vulnerable to expensive problems, lost data, viruses, hacker attacks and a host of other problems.

Connectability

What Every Business Owner Must Know About Hiring An Honest, Competent, Responsive And Fairly Priced Computer Consultant

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

21 Revealing Questions You Should Ask Any Computer Consultant Before Giving Them Access to Your Company's Network

Dedicated To Your Success
info@connectability.com | (416) 966-3306

Download your FREE copy today at
www.connectability.com/21questions/

Shiny New Gadget Of The Month:

'Peep' The World Around You

Peeps by CarbonKlean is the ultimate cleaning tool for glasses – far better than your traditional rag, spray or T-shirt. It's compact, easy to use and, most importantly, revolutionary in its ability to not only clean smudges off your glasses but also protect them from the next smudge.

Peeps uses state-of-the-art carbon molecular technology to remove smudges and dirt at a microscopic level as well as keep your lenses clear of contaminants long after you use it.

To clean your lenses with Peeps, simply brush them to remove dust and particles, wipe them between the heads of the tongs and enjoy your crystal-clear vision!

Why Secure Passwords Need Length!

The truth is, no matter how many times we see a warning about protecting our online identity, we take the easy route. It's like the verification box we're forced to check accepting the terms and conditions when we create a new online account, whether it's for Facebook or a bank account. At most, we skim through the agreement and hope that nothing bad happens. And this mentality applies to *everything*. Unfortunately, that means that most people take the same approach when creating passwords. Creating strong and hard to guess passwords is difficult, so most of us instead opt to keep it simple and hope for the best!

Passwords are an extremely important component of protecting your online identity. They are the first line of defense against unauthorized access to your accounts and confidential information. The more complex your password is, the more difficult it is for hackers to break in.

Traditional password practices include selecting a word and adding numbers, uppercase letters, and special characters. For instance, it could be your cat's name: Chl0e25@. Now, most of us would agree this password is complex, regardless of its length. However, the FBI has chimed in and clarified that longer passwords which include simple words and constructs, are better than short passwords with special characters.

A general rule of thumb is that your password should be at least 15 characters. The issue here is trying to remember multiple 15-character passwords. That's why we recommend using passphrases. Passphrases are a string of words, that make it harder for cyber criminals to crack, while also making it easier for you to remember. A passphrase uses spaces and symbols. It also doesn't have to be a proper sentence or grammatically correct. For example, it could be Chloe Luvs Her Yarn! What you use is entirely up to you but using passphrases can be a good way of locking down your accounts to prevent unauthorized access. In addition, to help remember all your passwords, you should consider using a password management program. There are many inexpensive and free password managers that use the same encryption as major banks.

To keep your business protected, it's important to use long and complex passwords. A password is the first "lock" on the front door of your business. If a hacker cracks this open, they can rummage through your personal information and cause chaos. Don't take the easy way out – use passphrases NOW!

Tech Connect Video Series:
Beware Of Phishing Attacks!

You probably spend a lot of time emailing clients, vendors, partners and colleagues. It's your main tool to communicate. Unfortunately it's also a hacker's prime target. Hackers use a method called "phishing" to convince their victims to open malicious links or attachment, send funds to random bank accounts, or provide confidential information about themselves or their companies. Cybercriminals can then get your passwords, install programs on your computer and network, and steal your confidential data.

Cybercriminals are working diligently to get into your computer, infect your backups, and install Ransomware across your network. That's why your business needs to stay up to date on the latest solutions and training to help your team spot phishing attacks, and prevent them from arriving in your inbox to begin with.

If you would like to learn more about improving your security and preventing your business from becoming a victim of a phishing attack, watch this video NOW! You will learn 3 tips to improve your email security. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video "**Beware Of Phishing Attacks! 3 Tips To Improve Email Security**" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

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

Earlier this year, the US 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.
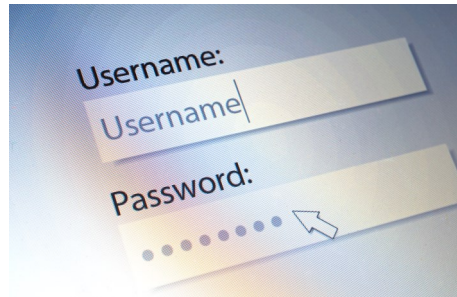
The Best Tips For Training New Hires

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.

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 gift card to Starbucks. Ready? Call us right now with your answer!

What popular social networking site was sold to News Corp. for $580 million in 2005?

a) Twitter
b) Myspace
c) Facebook
d) Snapchat

Call us right now with your answer!
(647) 492-4406

This month we will be donating to **The Salvation Army**.

Founded in 1882 in Canada, The Salvation Army is one of the largest non-governmental direct providers of social services. They are committed to giving hope and support to vulnerable people in 400 communities across Canada, and more than 130 countries across the globe.

The Salvation Army's focus is to provide aid for children and families, by offering necessities of life. The organization is dedicated to fighting homelessness and providing rehabilitations to those with addictions. The organization goes above and beyond to not only meet the needs of the individuals they serve, but to offer additional social and community service programs that focus on nurturing capacities, skills and strengths of the individuals.

If you want to contribute to The Salvation Army, we would love your help! Email: info@connectability.com or call (647) 492-4406.