ISSUE 54 JULY 2022

Newsletter

What's Inside:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

Co-Managed IT Services (CoMIT) - Empowering Your IT Team:

Many businesses deal with internal IT personnel that operate as generalists supporting the user community, the servers, then network and a whole list of additional duties; like line of business applications, cyber security compliance regulations, compliance, and staff training. For most businesses, the decision has been a hard choice of investing in inhouse staff versus the outsourcing to a professional Managed Service Provider. Today there are more options to consider by implementing a co-managed IT environment where internal staff and consultants work together by divide and conquer all the IT requirements for business efficiency.

An MSP brings capacity and a diversified expertise to the table, so your inhouse staff is assigned tasks according to what they do best, and you hire an MSP to focus on the skill sets that require a more unique level of experience, such as network management, cyber security, or compliance. Think of the benefits for your inhouse team to have readily available expertise to escalate issues to and mentor them through issues developing their skill sets. Meanwhile, as technology changes, you have expertise to rapidly implement new solutions at relatively the same cost of hiring and training new personnel and all the hidden costs there as well.

You now have a built-in buffer for downtime due to staff sicknesses, vacations, or replacement of staff. You now have a team that can come up beside the business while you decide your position on going forward.

Here are three situations where CoMIT will benefit your organization:

1. Your IT Staff is Limited in Size or Experience

Plenty of successful companies operate with one or two generalist IT staff in-house and occasionally need additional hands to meet the IT needs of the company. In addition, businesses can easily find themselves in positions where their internal resources cannot accomplish a given technology challenge or opportunity.

With CoMIT, small or larger size businesses can tap into additional workforce and expertise when needed.

For example, leadership could determine that in-house IT staff will focus on day-to-day tasks of employee operations while the MSP can be asked to manage the network operations and other duties that require unique skill sets, such as cyber security, while being available for escalations of the IT staff personnel.

Continued on page 2.

CONTINUED...

2. Your In-House IT Team is Overworked

SMBs can find its IT department is getting overworked, even larger in-house teams can find themselves in this situation. Seasonal swings, special projects and fast growth can all put additional pressure on existing IT teams.

CoMIT services allows businesses to bring in only the resources it needs when it needs them.

CoMIT services can also help relieve the pressure on a busy service desk staff. This helps prevent the tickets from piling up on the overworked staff and increases the response and resolution time for trouble tickets from other staff members.

3. Your In-House IT Team Lacks Experience with an Upcoming Project

With business strategy and technology in a constant state of change, businesses are often tasked with opportunities to implement new IT systems and programs. Existing in-house IT teams may not have the experience needed to successfully plan, implement and/or maintain an upcoming initiative.

CoMIT services can provide businesses with a broad range of experience and deep bench of experts beyond that of the existing in-house staff. Good MSPs are regularly sending their engineers to continuing education courses and encouraging them to get professional certifications. Also, due to working with various clients, they have also seen and worked through all kinds of issues, which are valuable learning lessons. These are strengths businesses can tap into with co-managed IT services.

Featured Partner:

Saaslio

Saaslio is the SaaS discovery solution that allows us to uncover, manage, and secure your critical SaaS ecosystem & the sensitive data it contains. By providing visibility into the cloud-based applications your team is already using, Saaslio helps us uncover and address vital security risks to your organization.

RJ2 SPOTLIGHT

Megan Muzzillo

Project Coordinator

Megan has been working in customer service for 4 years. Before joining the RJ2 family, she worked at Lifetime Fitness, where she gained experience and worked in higher management roles for multiple departments, including account management and customer service. She is currently enrolled in school to finish her degree in the management field. Megan joined RJ2 Technologies full time in October of 2019. She holds the rule of Support Specialist in the Administration Department.

Fun Fact: Megan was a Student Ambassador for People to People International that was established by President Dwight D. Eisenhower, as part of the United States Information Agency. She has been to China, Italy, Switzerland, Austria, and France.

Where's your favorite place in the world?

- That's a hard one! I love to travel and to be outdoors. I would have to anywhere traveling and seeing beautiful sights. My favorite places include: the places I traveled to in Europe and China. I would also have to include Colorado, California, and downtown Chicago (of course!).

What do you like to do when you aren't working?

- Enjoy spending time with friends, family and my two dogs. I also love to read, garden and practice yoga.

What is the best career lesson you've learned so far?

- Be confident, but humble and to embrace failure.

If you could meet anyone in the world, dead or alive, who would it be and why?

- My great-grandfather on my father's side. I would love to hear his personal stories about his life in Italy, his travels when immigrating to the United States and about his life when he first got here. I have heard many stories growing up, but it would be amazing to hear it from him.

What is your favorite part of working at RJ2?

- My coworkers, our clients and all the knowledge and experience I have gained while being here!

Working Remotely? Follow These Cybersecurity Tips:

Since the start of the pandemic, many businesses having been making the push towards remote/hybrid work environments. While this is a great feature for employees and allows for more flexibility; it also comes with some security risks. Check out these cybersecurity tips to better protect yourself, your personal information, and your organization's data.

Patch Your Software Regularly

While many of us may be tempted to push off a software update due to the annoyance, these updates typically include patches to critical weaknesses that will help protect your system from the newest threats. Many apps now offer an automatic update feature, so you do not have to manually patch your software.

Fortify Your Accounts

When allowing your employees to work from home, user accounts must be adequately secured. One way to do this is by setting company-wide password policies. Your passwords should be a minimum of 12 characters long, with a combination of both numbers and special characters mixed together to increase security measures. Make sure that your passwords are unique to every account to decrease the damage if hackers do happen to get into one employee's credentials. If you find it difficult to remember passwords or use the same password for every login you have, you might want to consider investing in a password manager such as IT Glue.

Use a Virtual Private Network (VPN)

VPNs are typically used to find a way around geographic limitations on location-specific websites and steaming services, but it is also a vital tool for remote workers. VPNs help protect you while on the internet by creating a secure connection between devices through the use of encryption. This will help hide your employees web activity from potential peaking eyes, which secures their online privacy and mitigates the risk of potential hackers getting a hold of your business's information.

Set Up Firewalls and Antivirus Software

Make sure your business is enabling quality firewalls in your operating systems and hardware. Firewalls offer a strong layer of protection between your devices and the internet, which will help to prevent malicious content from reaching you and your employees. MSPs (managed service providers) may also provide third-party firewalls in case your computers don't have any built in by default.

Your business will also want to invest in and implement antivirus software to detect and remove any sort of malicious programs that do happen to infiltrate your device. As mentioned earlier, remember to make constant updates to your software so it can effectively detect the newest types of malware.

Secure Home Routers

Home Wi-Fi routers are not as well protected as their business counterparts so make sure to take some extra precautions in securing them. The first thing you will want to do is change the default password as soon as you are finished setting the router up. Hackers can easily look up the default password online once they have determined what your router model is. Another good practice would be to install the latest firmware updates to eliminate any security vulnerabilities.

Lastly, confirm whether your router has Wi-Fi Protected Access 2 (WPA2) encryption settings to secure the inbound and outbound traffic coming through. If your device does not have this capability, it may be time to start searching for some router upgrades.

Back Up Your Data

Your business should be making consistent backups to ensure that you will always have access to your important data in the event of a disaster. All businesses should be prepared for the worst, especially if your business cannot afford much downtime. For more information on backing up your data visit RJ2's Backup & Disaster Recovery Page.

Watch For Online Scams

The biggest threat that remote employees face is online scams. In general, most attacks that happen to a business are a direct result of human error. This could be employees clicking on phishing emails or entering credentials into a spoofed webpage. Either way, it is important that your employees have some training in identifying potential malicious content.

To avoid these kinds of threats, you must be critical of everything you come across on the internet. Look for suspicious links and attachments, grammatical errors in the URL, misspelled emails, etc. Also, you should never give out your sensitive information through an email, text, or phone call.

Working remotely can be a great option for your business and offer your employees more flexibility. However, there can be many security challenges that come with supporting remote work and your business needs to make sure that you are taking the proper precautions. For more information on how a managed service provider such as RJ2 can protect you from cybercrimes, get in touch with us today by clicking here.

How SaaS Can Benefit Your Business:

Businesses across the world rely on various types of software to streamline and improve their daily operations and the successful businesses are constantly searching for faster and cheaper ways to get things done more efficiently. One way to do this is through utilizing Software-as-a-Service (SaaS), which enables you to obtain the necessary software in a budget-friendly manner. Learn more about how SaaS can benefit your business while also saving you money.

What is SaaS, and How Does it Work?

Not too many years ago, the main way to get software installed on your devices was to either buy a physical CD or directly download the software through the internet. This software then needed to be installed on the users' machines which meant they had to have a significant amount of storage capacity and processing power to efficiently run the software. Not to mention, the user also had to purchase a license for the software copy which was typically limited to one license per machine. This meant if the user wanted to have multiple copies of the software on different machines, they would have to pay twice for it.

In the business world, software delivery was streamlined so that on-premises (on-prem) servers held the software programs, and users accessed these programs via the company's intranet. The user's own devices acted as mediums for entering input and displaying output, but most, if not all, of the processing was done by the on-prem servers. With this type of setup, economically priced license packages allowed business to obtain a single software copy that could be efficiently used by hundreds of users at a time.

Today, SaaS essentially allows you to go on the internet, and "borrow" the machines of a service provider to access the different types of software applications installed on those specific machines. Since the software is installed on the service providers machines, the user will only need an internet connection to access the SaaS apps. Now, users can use different types of software applications on the go through their mobile devices as long as those said devices are connected to the internet. This means employees can effectively work from home and not have to be in office to access applications.

Should You Switch to SaaS or Stay with On-Prem?

SaaS would be the ideal solution for those looking to reduce their costs. With on-prem software, businesses would first need to buy the hardware, which needs to be maintained to ensure proper functionality. Next, you will need to purchase the software license and pay yearly support fees, which can get rather expensive compared alongside the costs of using SaaS.

With SaaS, you only need to pay a monthly or annual subscription which gives you access to that server's software applications. Since the cost is cheaper to pay on a monthly or annual basis, this allows users to diversify their software applications in multiple SaaS platforms.

How Flexible is SaaS?

On-prem solutions used to have two main advantages over SaaS: first they were granted more functionality and second, they used to be more customizable. However, SaaS vendors today are constantly introducing new features to make work easier for their users. Also, businesses have the ability to integrate SaaS apps with other apps so suit their needs. This means if one of the applications is missing a specific feature your business needs, you can find another app designed for that specific feature and use both services.

Is it Safe?

Organizations often cite data security concerns as reasons for not adopting SaaS. Will the company's data be safe? Who will own such data? What if the SaaS vendor's business goes kaput?

These are all valid concerns. But you should know that the average SaaS vendor invests more in cybersecurity, backup tech, and maintenance than the typical small- or medium-sized business. This is the vendor's line of business, and they can't afford to lose their clients' trust.

Moreover, they're subjected to strict security audits, especially those that are covered by data regulations like HIPAA.

Additionally, when your organization takes on a SaaS vendor, both parties sign a service level agreement (SLA). This SLA has clauses specifying who owns the data inputted into a program and the output produced by the program, and the vendor's obligation to grant you access to your data even if they suffer economic setbacks or business failures.

For more information on SaaS, send us a message today. We'll help you determine if utilizing SaaS is best for your business.

Tech Tips of the Month:

- Utilize Multi-Factor Authentication (MFA) to add another layer of security protection to your data.
- Never click on links if you aren't sure who the sender is.
- Don't use the same password for every account. This way, if one account is hacked, your other accounts will still be protected.
- Avoid saving your passwords to internet browsers
- Install antivirus/anti-malware protection.

What’s the Difference Between HDD and SDD?

Hard disk drives (HDD) and solid state drives (SSD) are the two main types of storage devices you should consider. When comparing the two, there are a few different factors to consider such as speed, capacity, cost, durability, and noise. While hard disk drives (HDD) have been around longer, both types of storage devices have unique features.

What is an HDD?

An HDD is a small storage device that is sits inside the computer and records data by reading and writing on a disk where the data is then stored magnetically. The inside of the device looks similar to an old record player, where there is a platter or stack of platters rotate around a needle, and an armature called a read-write head. The data is then stored on the platter using very small magnetic particles.

What is an SSD?

An SSD differs from a HDD because it does not have any internal moving parts. It instead uses integrated circuit assemblies to store, retrieve, and cache data. The two main components of an SSD are: the controller and flash memory chips. Flash memory contains storage memory, while the controller executes firmware-level software.

HDD Vs. SSD: How Are They Different?

We’ll compare the two storage devices based on these five categories.

1. Speed

HDDs take a long time to access data because the disk must spin to find it. They typically have a spinning speed of around 5,400 to 7,200 rotations per minute.

In contrast, SSDs can complete the same task 200% faster since they rely on instantly accessible memory chips. That’s why a computer equipped with an SSD can boot an operating system and load apps much faster than one that uses an HDD. An SSD can copy and move large files at 500 MB per second, while an HDD can do the same at 30–150 MB per second. This means you can copy a 20 GB movie in less than 10 seconds with an SSD, but you would need at least two minutes with an HDD.

2. Capacity

Thanks to recent technological advancements, SSDs can now support terabytes of storage, just like HDDs. However, if you compare today’s lowest-priced laptops, you’d see that they’re either equipped with 128 GB SSD or 500 GB HDD. Why is there such a huge difference in storage capacity? It’s because SSDs come with prohibitively high price tags. Therefore, if you require a lot of storage space, HDD is the way to go.

3. Cost

For the same storage capacity, HDDs are less expensive than SSDs, which is why they’re often bundled in budget laptops and PCs. To keep its price competitive, a budget laptop typically can have only up to 512 GB SSD storage.

Some gaming laptops solve this speed-price dilemma by having both an SSD and an HDD — SSD for key applications and HDD for data. However, take note that most consumer and business laptops do not have room for multiple storage drives. Fortunately, you can easily find 1 TB external USB hard drives for under $50.

4. Durability

HDDs are more susceptible to shock and damage because they have various moving parts and components. This means that if you accidentally drop your laptop, your HDD might get damaged and your data will be lost. Moreover, the longer you use your HDD, the more it wears down and eventually ends up failing.

In contrast, because SSDs use a nonmechanical design of flash storage mounted on a circuit board, they are more durable and are better at keeping your data safe.

5. Noise

An HDD emits some noise when the drive spins back and forth to process data. In contrast, SSDs do not have moving parts so it does not make any noise at all.

Conclusion

Overall, SSD is the clear winner over HDD. While more expensive, SSD is the faster and far more durable data storage option in the long run.

If your computer can support multiple hard drives, you can use an SSD as the primary storage for your OS, applications, and most-used programs. You can then use an HDD to store pictures, documents, and other files that do not require quick access times and speeds.