PALMTECH
I.T. Solutions For Business

# THE PALMTECH TIMES

PalmTech Computer Solutions July 2021

## In-House IT vs Outsourcing IT

Are you a business owner trying to decide between housing an internal IT branch or outsourcing IT to a managed service provider (MSP)?

Chuck Poole, PalmTech's CEO, recently added an article to our blog which will guide you through the pros and cons between the two types of service models in an honest and transparent fashion.

**Visit:**
www.palmtech.net/comparison

**If you have any questions, call us at 561.969.1616!**

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

### Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

# These Technologies Hold The Key To Growing Your Business

After a roller coaster of a ride in 2020 and into 2021, businesses just like yours are looking to the future. Their eyes aren't just on recovery. Many businesses are eager to make up for lost time, and they want to bring new customers into the fold.

There are countless growth strategies out there, but one area offers a lot of options you can dial into your specific business needs: technology. Under the umbrella of tech, you have plenty to choose from. It really comes down to finding the right solutions that fit the current or future needs of your business.

This month, we'll dive into two ways you can utilize various technologies to grow your business in the second half of 2021 and in the years to come. Let's get started.

### Using Automation

Many businesses have yet to crack the code on automation. They aren't sure how to implement it and make the most of it. And that's okay. Automation comes with a few hurdles, like just getting started for one. It's an investment of time and money. However, once you get started, it does the rest.

A majority of daily business activities can be automated. One increasingly popular form of automation is artificial intelligence (AI), often used by chatbots. In the past, chatbots were useless. From the user standpoint, they never worked as expected. But those days are over; thanks to major strides in AI technology, chatbots are automation kings.

Chatbots are highly customizable. You can use them as the first "person" a customer or potential customer sees when they visit your website. From there, a chatbot can ask questions and mimic a real person. But here's where the automation really comes into play: if a potential customer has a specific request or question, the chatbot can instantly direct them to the person within your company who can help. It saves a lot of time.

*continued on page 2*

Automation is also useful when it comes to collecting data. Now, you can rely on numerous apps to collect different types of data and have it all sent to one place. For instance, you should have forms on your website where people can input data, such as their name and e-mail (and other similar data you may be interested in). You lock free content (such as special reports, books, videos, demos, offers, etc.) behind a "data wall." Once a potential customer gives you what you want, they get access and you have a lead.

**Investing In IT Security**

Many businesses went through huge changes last year. One common change was the shift to remote or hybrid work models. In the process, these businesses had to figure out a lot of things on the fly, from how to get their employees up and running to making sure their data was secure.

Unfortunately, many businesses, particularly small and medium-size businesses, struggled to balance getting their employees up and running and staying secure, due to a lack of resources, support or know-how. They ended up having to focus on one or the other – data security often got left in the dust. And in the mix of it all, growth completely fell off their radar.

We're going into Q3 2021, but many businesses still lag behind when it comes to their IT needs. Not investing in network security, and an overall IT security strategy, has the potential to hold your business back and prevent the growth you're looking for. Not only is your data at risk from both internal (hardware failure, data loss, etc.) and external (data breaches, cybercriminals, etc.), but there are also other issues to be aware of.

Here are a few questions to consider:

- Do your employees have strong endpoint security? (Are their devices and network connections secure?)
- Are they trained in IT security protocols? (Do you have protocols in place?)
- Are your network and IT needs scalable? (Do they allow for growth or are they static?)

These questions are a starting point. If you aren't happy with the answers, it's time to fill the gaps and give your business the advantage it needs for the future.

**Getting Started**

If technology still eludes you, you want to jump into the cloud or automate parts of your business, or you need to boost your data security, your best next step is to partner with a managed services provider (MSP) or a firm that specializes in IT solutions. You never have to do any of these things on your own – especially if you have questions or aren't sure how to get started. This is the kind of partnership that can put your business on the path to hitting your growth goals and set you up for tech success!

**Contact PalmTech with questions, concerns or to obtain more information on our managed IT and security solutions—561.969.1616 or info@palmtech.net.**

**"There are countless growth strategies out there, but one area offers a lot of options you can dial into your specific business needs: technology."**


## Are Your Employees' Credentials For Sale On The Dark Web?

**Visit www.palmtech.net/darkweb/ For A Free Scan!**

# Tips To Keep Your Business Data Safe

Losing or compromising data can be disastrous for your business. It can lead to reputational damage, costly lawsuits, and termination of contracts, among others. And because threats to data security are always present online, it's important to implement tough security measures that will keep your business data safe 24/7. Here are some tried-and-tested methods to safeguard your corporate data.

### *Use Multi-factor Authentication*

Using a complicated password to secure your system is not an effective way to level up your cybersecurity. That's because having to memorize a difficult password often pushes users to set that same complex password for multiple accounts. And if a hacker gets a hold of a recycled password, there's a high probability that they could access all your accounts that use that same password.

Two-factor authentication (2FA) adds an extra layer of security to your systems and accounts. 2FA comes in many forms: it can be a biometric verification in the devices that you own or a time-sensitive auto-generated code sent to your mobile phone. This security feature works similarly to how websites would require you to confirm your email address to ensure that you are not a bot.

### *Encrypt All Data*

Encryption is an effective obstruction to hackers, since it scrambles and descrambles data every time someone tries to read it. Encryption also causes compatibility issues if the data is not being accessed via a company's own network systems. While applying encryption can be expensive, it is certainly well worth the money because it protects your data in case it falls into the wrong hands.

### *Keep Systems Up to Date*

Hackers are always upgrading their tools to take advantage of outdated security systems, so companies should keep up to protect their valuable technology resources. Many companies don't install software updates immediately, and that's a huge problem. Updates often close existing security loopholes, which is why delayed installation can mean exposing your systems to external attacks. Keep your data safe by installing software updates as soon as they are released.

### *Back Up Frequently*

Implementing several layers to your security doesn't ensure that hackers won't find their way into your systems. This is why you need to back up data frequently, whether it's on-site, off-site, or by way of cloud backups. In the worst-case scenario where your systems *do* get infiltrated, you can restore lost data from your backups.

### *Monitor Connectivity*

Many businesses have no idea how many of their devices are connected online at a given time, so it's very hard for them to keep track of which of these should actually be online. Sometimes, a company's computers and servers are online when they don't need to be, making these tempting and easy targets for attackers. It's advisable to configure business servers properly to guarantee that only necessary machines are online and that they're well-protected at all times.

**It's much more expensive to recover from a data breach than to prevent one.** If you're looking to protect your business IT systems from potential threats, contact us today so we can help at **561-969-1616.**


**"I DIDN'T KNOW"**

Unfortunately, that excuse doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

**Sign Up For Our FREE "Cybersecurity Tip Of The Week" and Always Stay One Step Ahead Of Hackers and Cyber Attacks!**

**Visit: www.palmtech.net/weekly-tips/**

**You Must Constantly Educate Yourself On How To Protect What's Yours!**

# How Much Could A Ransomware Attack Cost You?

Have you ever thought about how much your data is worth? Information is possibly the most valuable part of your business – there's your client database, accounting software and inventory management, and of course, any intellectual property you may own.

When ransomware hits, businesses are suddenly forced to re-assess the value of their data: is it worth saving, and what's the deeper cost of the attack?

Most ransomware attacks cost $150-$600 to get your files released, but that's only IF the cyber-criminals honor the payment and actually give you the decryption key. Meanwhile, new client calls are still coming in and you may find yourself unable to operate with your systems down. Paying the ransom or restoring from an unaffected backup seems like a quick fix, but it doesn't end there. There's still the downtime involved to restore all your data – possibly days – and that's a lot of lost productivity.

Plus, if word gets out that your data has been compromised, you may find confidence in your business plummets and your existing clients head elsewhere. That $150 ransom may end up costing well over $150,000!

### Prevent Ransomware Attacks on Your Business

**Keep Your Systems Up to Date:** Many ransomware attacks take advantage of flaws in older versions of Windows, ones that have since been patched by Microsoft. But to be protected, businesses must be up to date with their patches AND be running a supported version of Windows. Delaying patches and updates puts your business at risk - we can help you update automatically.

Lock down employee computers: Very few staff will require full administrator access to your business network. The higher their level of permissions, the more damage a person can do – either accidentally with a whoopsie click, or by inadvertently installing malware. By locking down your employee computers, you have a better chance of containing a malware attack to non-vital systems. Our experts can design an access management plan that gives you best of both worlds: **flexibility PLUS security**.

**Educate Your Workplace:** Most employees believe they're being cyber-safe but the reality is quite different. Many malicious links and embedded malware have become hard to spot in an instant – which is all it takes to click and regret. We can work with your staff to establish procedures around checking links for authenticity before clicking, awareness around verifying the source of attachments, and the importance of anti-virus scanning. We'll help get the message through!

**Have a Solid Backup Plan:** When ransomware hits, a connected backup = infected backup. Unfortunately, synced options such as Dropbox immediately clone the infected files, rendering them useless. The only safe backups will be the ones both physically and electronically disconnected, with systems designed to protect against attacks like this. Our experts can set you up with a backup system that makes recovery a breeze.

**Be Proactive:** The best way to avoid the financial cost of a ransomware attack is to prevent it from happening in the first place. Smart businesses are the ones watching these widespread ransomware attacks from the sidelines, completely unaffected and seizing opportunities while their competitors are down.

**Our managed services can help protect your business against the next cyber-attack. Call us today at 561-530-2948.**


*"My email is down, so if you need to communicate with me, use this."*

CartoonStock.com