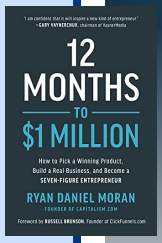
PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions May 2022

12 Months To $1 Million
by Ryan Daniel Moran



While first starting your entrepreneurial journey, you'll come across many sources that claim to give you an "easy path to success." Considering the fact that more than half of all businesses close within their first six months, it's safe to say that there is no easy path to success. Instead, it takes plenty of hard work and dedication to run a successful business, especially if you hope to reach the $1 million mark. In Ryan Daniel Moran's book, 12 Months To $1 Million: How To Pick A Winning Product, Build A Real Business, And Become A Seven-Figure Entrepreneur, he explains that it is possible for your business to reach the $1 million mark within the first year by following his plan. He'll take you through step-by-step and explain how to grind, grow and reap the benefits from your hard work.

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.

Stay Compliant
By Upping Your Cyber Security

If you own or operate a business, there are plenty of things you must do to ensure success. You have to make the right hiring decisions; develop a product or service that you can sell; build relationships with clients, employees and partners; and much more. One of the biggest responsibilities that comes with owning or operating a business is ensuring that your business is compliant with any guidelines put in place by regulatory bodies.

Every business needs to make an effort to stay compliant, and a big part of that is making sure your cyber security practices are up to standards. With technology rapidly advancing and regulations changing fairly often, you have to stay up-to-date on any changes that should be made going forward. You also need to make an effort to plug any holes in your current cyber security plan.

You can do this by asking yourself a few questions and making the necessary adjustments if you answer no to any of the following:

- Is my business protected by a firewall and antivirus software?
- Do I use backup solutions, and do I have a disaster recovery plan in place?
- Has my storage stayed up-to-date with any technological changes?
- Do I have any content or e-mail spam filtering software?
- What data am I encrypting?

Ensuring that your business stays compliant will be extremely important in maintaining client and employee relationships. If a customer's information gets compromised because your business did not have the necessary cyber security in place, they probably won't come through your doors again. As technology changes and evolves, so do many of the regulations and cyber security practices that you should put in place. It can be difficult to become compliant if your business was lacking previously. Luckily, there are a few steps you can take to

continued on page 2

help ensure that your business becomes and stays compliant with any regulating bodies.

First, you should document all of the consumer data your business holds. If a customer asks what information your business has collected on them, then you should be able to give them an honest answer. You might also be obligated to share this information. By keeping and maintaining this information, you will be able to supply your customers with it if they ever do ask.

It can also help greatly to partner with a managed services provider who manages IT needs since they will be able to perform routine IT data checks and work to better protect your customer and the private information within your business. MSPs go a long way toward helping all of your potential IT needs, but their usage when it comes to cyber security, protection and compliance should not be underestimated. Partnering with an MSP will help get your business on the fast track to becoming cyber-secure.

Another big part of ensuring that your business stays compliant is to introduce cyber security training for all of your employees. Did you know that 95% of cyber-attacks start with human error? If your team has not bought into a cyber-secure culture or does not know the proper cyber security practices, you could be in some trouble. Make sure that cyber security training is part of your onboarding process and continue to train your employees throughout their tenure with your business.

"Cyber security and compliance work right alongside each other."

Once your employees are aware of the risks of cyber-attacks and have bought into a cyber-secure culture, it's time to upgrade your cyber security. One of the best things you can do for your business is to invest in regular software patching. Technology is ever-evolving, and we should make the necessary changes to ensure it continues to cooperate with our network and systems. Put technology in place to cover these holes or partner with an MSP that can help take care of any lapses in your cyber security.

Additionally, you should invest in some content-filtering software. There are plenty of toxic websites with nefarious intent that can wreak havoc on your cyber security if accessed by an employee on your network. Content filtering allows you to restrict certain websites. It also goes a step further by recognizing patterns in websites that have malicious codes and blocking those websites that might pose a risk.

Cyber security and compliance work right alongside each other. If you're trying to ensure that your business stays compliant, you need to buff up your cyber security practices. There are many methods you can take to do this, but if you're unsure of where to begin, give us a call at **561-969-1616** or email us at info@palmtech.net. We would be glad to help you take the next steps toward creating a cyber-secure business.

Free Cyber Security Assessment

Cartoon of the Month

10 Habits To Ensure Equality In Your Hybrid Team

Businesses across the country are switching over to hybrid work environments. If you're in this boat, you may be wondering how to keep things fair between your remote and in-office employees. Below you'll find 10 habits to implement that will create an equal environment for all of your employees.

Change How You Track Productivity: When you work in an office, many consider "working" to simply mean being in a work environment. If you have a hybrid team, you need to come up with a new system to track productivity. This measurement should be based on output and results.

Standardize Your Meetings: It can be awkward and frustrating for a remote employee who can't hear or see what's going on during a meeting due to poor camera angles or audio issues. It can help to have your entire team meet on Zoom rather than just those who are working remotely.

Use Public Channels: Use public channels like Slack or Microsoft Teams for communication between your team to ensure everyone is in the loop.

Digitize Your Resources: You need to have digital resources readily available for your remote team members because they can't simply ask their nearest coworker or check office records for information.

Keep Remote And Office Workplaces Consistent: You may have spent a lot of money designing your workplace but you also have remote employees who may be working in cramped spaces. Make sure your design principles extend to your remote employees. This will help so that productivity, safety, training and brand representation will all remain consistent.

Diversify Company Rituals: Many businesses focus on creating a company culture, but this becomes difficult with remote and in-office employees. You need to make sure your company and team-building rituals include everyone.

Equal Rewards: There should not be a difference between the rewards your in-office and remote employees receive. Make sure you are acknowledging your remote employees on public channels and sending them gifts or perks since they can't participate in team lunches.

Coordinate Team Schedules: If you have employees coming and going from the office at all hours of the day, communication can get fuzzy. Try to keep your departments' schedules lined up so people can still use one another as resources.

Repeat Important Announcements: Your remote employees will not be in the break room hearing about everything that's happening in the office. You need to keep them informed of any ongoing developments with the business or other major announcements.

Seek Feedback: You should always try to get feedback from your remote and in-office team members so you can make necessary adjustments. The experience needs to work for all of your employees, so feedback is critical.

By putting some of these tactics into action, your hybrid team will be working more cooperatively and efficiently than ever before.

Laurel Farrer is the president of the Remote Work Association and CEO of Distribute Consulting. She specializes in advocating for the impact of workplace transformation on corporate and economic growth.

'I DIDN'T KNOW'

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines

It's coming ...

- That day a hacker steals critical data, rendering your office useless
- That day when your bank account or credit card is compromised
- Or that day when your customers' private lives are uprooted

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

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE "Cyber Security Tip of the Week." We'll send these byte-sized quick-read tips to your e-mail inbox. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

Get your FREE "Cyber Security Tip Of The Week"
https://www.palmtech.net/resources/cyber-security-tip-of-the-week/

Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo and Target Did?

If the answer is "NO" – and let's be honest, the answer *is* no – you are leaving yourself and your company open to massive liability, ***millions*** in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time before they destroy your business, scare away your customers and ruin your professional and personal life.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Get your free Dark Web Scan TODAY at www.palmtech.net/darkweb/

Our 100% FREE and 100% confidential, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers.

*Reserve your exclusive CEO Dark Web Scan **now**!*

What Is Data Privacy?

In simple terms, data privacy means ensuring confidential information remains confidential. The goal of data privacy is to provide a path for organizations to legally collect information, while prioritizing individual rights to privacy. In order to achieve that goal, data collectors must implement security procedures that determine what data gets collected, how it's collected, how it's stored and transferred, who has access to it and, most importantly, how it's protected.

For example, many organizations collect personal data about their clients and customers, including full names, financial information, health information, national ID numbers, and so on. Failure to protect this data could result in hefty fines, costly legal action, and could also permanently damage an organization's reputation with business partners and customers.

The consequences are just as bad for anyone whose privacy was compromised. Imagine receiving an invoice for a service you didn't subscribe to, or discovering inquiries on your credit report that you didn't authorize. This is known as identity theft and it's a direct result of failed data privacy.

Privacy vs. Security

Privacy and security work together, and often get interchanged in casual conversation. But there is an important difference between the two. ***Privacy refers to the appropriate use of any data that is collected, stored, and transmitted.*** For example, posting someone's private information on Twitter would be a violation of their privacy.

Security needs to be an ongoing commitment to preventing unauthorized access, both externally and internally, to confidential information. Security combines technical measures, such as firewalls, spam filters, and threat monitoring software, with human measures like following policy and thinking before clicking. If you haven't implemented such measures and you have confidential personally identifiable information on others, then you and your company are vulnerable.

- SAC