PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions July 2022

Start From Zero

By Dane Maxwell

If you've picked up a business book over the last few years, you may have read chapters encouraging you to improve your skills. Not everyone shares the same skill sets, nor do we all have access to an equal amount of funds. So, how do you start a successful business without any of the necessary skills, resources or even confidence? That's where *Start From Zero* is able to help. Dane Maxwell takes readers on a learning journey to help them realize that success is within themselves and that anyone can become a successful entrepreneur by following his tips, regardless of their background. *Start From Zero* is an essential read for any new business owner who is dipping their toes into the entrepreneurial pool.

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.

Do I Need A Compliance And Cyber Security Plan?

We talk a lot about cyber security and how incorporating the right practices can help fully protect your company from cyber-attacks, but there's another term that's often referenced when discussing cyber security that's just as important: compliance. While it's incredibly important for businesses to focus on maintaining the highest cyber security standards, they also need to ensure protocol meets compliance standards.

In regard to cyber security, compliance means creating a process to help protect the confidentiality and accessibility of information that's stored, processed or transferred. There is not an overarching standard for compliance when it comes to this. Instead, there are different guidelines and requirements for every industry, so it's important to be aware of your company's needs. If you're not, you could be subject to fines and penalties in addition to being at greater risk for cyber-attacks.

Though they're related, there are still some glaring differences between cyber security and compliance. Cyber security is practiced for the company's own sake instead of to satisfy the needs of a third party. It's also present to protect a business from the risk of constant threats and needs to be continually managed and updated. IT compliance, however, is completed to satisfy external requirements and is driven by what the business needs more than anything else. Unlike cyber security, compliance is finished when the third party is satisfied with your process.

Compliance and cyber security work best

continued on page 2

when they're aligned, so it's extremely important that your business has a plan for compliance and cyber security. On its own, compliance is incredibly important for various reasons. The first is probably the most obvious since you can be fined or penalized if you fail to comply with industry standards. Having the proper compliance program will prevent your company from being fined. Additionally, your compliance plan needs to include continuous monitoring and assessment of networks, devices and systems that your company uses in order to align with regulatory cyber security requirements. It also sets up an action plan if your business is ever breached, since you need to communicate news of the breach to any parties that could've been impacted.

Every business, regardless of size, is susceptible to data breaches. It's only with strong cyber security and IT compliance plans that you can hope to plug every hole hackers may look to exploit. Compliance is an important part of risk management, and it's essential for the future success of any business.

A compliance plan alone is a great start, but having cyber security measures in place as well will help you be prepared if you're ever audited by a third party.

Whether you have teams or individuals who oversee security protocols, they all need to know the requirements for cyber security compliance and exactly how protected the company is. If your company utilizes a firewall, which it absolutely should, your teams need to know exactly how protective that firewall is. They also need the evidence to back up their claims so they can prove the information they provide is accurate. Auditors want to see a handful of different documents, so make sure your team is prepared for any questions or requests.

Once you have the basics of your plans taken care of, you can focus on accurately documenting each step. From meeting notes to the list of items that an auditor may need, your entire team needs to document anything they do or see regarding cyber security.

There is another, much easier option to ensure your business stays compliant and is protected from cyber-attacks. You can hire a managed IT services provider. With a managed IT provider, you will have a dedicated team that ensures your company's sensitive information is protected and all of your cyber security holes are filled. They'll also ensure your business stays compliant with any third-party regulating bodies in the process.

Though technology is ever-advancing, you shouldn't have to worry about cyber-attacks on a daily basis. With strong security protocol, or with the help of a trusted managed IT services provider, you can rest easy knowing your company's information is as secure as possible.

Cybersecurity Myths, Busted!

It's time for a pop quiz: Which of the following is a myth?

A. Only people in high-power positions are targets of cybersecurity attacks.

B. High-tech hackers pose the highest threat to your organization.

C. Cybersecurity is a highly technical process that only your IT department can handle.

D. Security awareness only really matters when you're at work.

E. Smart devices are rarely targeted by cybercriminals.

Did you find the myth? Hopefully you did, because this was a trick question! Each of these is a common cybersecurity myth. Read on to learn the truth behind these misconceptions:

Myth #1: Only people in high-power positions are targets of cybersecurity attacks.

Executives and administrators are prime targets for cybercriminals, but that doesn't mean they're the only targets. Scammers attack every level of an organization, looking for gaps in security. After all, it only takes one hacked machine to access your entire network.

Myth #2: High-tech hackers pose the highest threat to your organization.

You may imagine a cyberattack as the use of highly sophisticated technology to break down firewalls and decode user passwords. But in truth, it is much more likely that Dave wrote his password on a sticky note and it fell into the wrong hands. Human error is an easy target for cybercriminals, so stay alert!

Myth #3: Cybersecurity is a highly technical process that only your IT department can handle.

The security tools that your IT department manages are important, but technology can only do so much. These security measures can't stop an employee from sending sensitive information within an email. Creating a human firewall, made up of each and every employee, is essential to the security of your organization. Security is everyone's responsibility.

Myth #4: Security awareness only really matters when you're at work.

Your organization's at-work policies and compliance regulations may not be necessary in your home life, but security awareness still matters. Scammers could phish your personal email for bank accounts, login credentials, or even personally identifiable information, which can be used to perform identity theft.

Myth #5: Smart devices are rarely targeted by cybercriminals.

Nearly everyone has a smartphone and many people use smart devices throughout their homes. From smart speakers to security cameras to lightbulbs, all of these gadgets connect to the internet. As these devices become the norm, cybercriminals happily accommodate. Treat smart devices the same way you would treat any other computer. Always use strong passwords, install antivirus and anti-malware software, and keep these devices up-to-date with the latest security patches.

Believe it or not, you are the key to keeping your organization secure!

For more information on our Security Awareness Training, contact us at **info@palmtech.net** or call us at 561.969.1616.

PalmTech TidBits

The Future Of Leadership

The pandemic completely changed the way many people view work. If there's one thing for certain, it's that remote work will continue once the pandemic ends. If your business has switched over to a remote or hybrid environment, you may need to reevaluate your leaders to ensure their skills align with the new work environment. Strong remote leaders possess traits that are essential for success.

In fact, if you want your business to prosper in the future, you must ensure your leaders are good communicators since they might not be working in the same location as their employees. They also need to possess collaboration skills to ensure each facet of every project is covered. Additionally, your leaders should be able to align their values with those of your staff and customers. Empathetic and understanding leaders are the future, and you need to have a leader who will look out for their team while also taking care of any customer needs. If you interview a candidate who possesses these great characteristics, they should be a top contender for your leadership positions.

Reasons Your Business Should Be Using a Private Cloud

Gone are the days when everything was stored on a physical hard drive. Now, most businesses and private users utilize cloud computing to store their data. It's no secret that cloud storage is the present and future of data storage, but have you thought about using a private cloud that only allows your business and permitted users to access necessary information? There are many benefits that come with using a private cloud, such as the following:

- It offers better security since nobody besides authorized users can use the storage or servers.
- Your team will gain greater flexibility to continue their work without the fear of IT issues since backups are done automatically on private cloud servers.
- It's often cheaper to use a private cloud than to maintain physical servers.
- Private clouds usually come with managed IT services, so there's no need to hire an IT team to work on-site. This will save you time and money.

Steer Clear Of Fake Login Pages

For cybercriminals, stealing your login information can be just as valuable as stealing your bank account information. If they gain access to your email and password, they may find clues in your account that they can use to create highly targeted phishing attacks against you, your organization, or your family. Once the hackers have your login information, the hackers can even sell it for payment.

How Does It Work? A popular method used to steal your credentials is to use fake login pages to capture your login details. These types of attacks usually start with a phishing email that directs you to use a link in the email to "log in to your account". The emails are usually authentic-looking and present a seemingly normal request. If you click this link, you're brought to a login page that looks almost identical to the one you're used to but is actually a fake page. Once you've entered your email and password on the fake page, you may be redirected to the real website–leaving you unaware that your login credentials were stolen.

How Do I Spot a Fake Page? As the first line of defense, always navigate to your account's login page by typing the web address in your browser, or using a bookmark that you've saved–rather than clicking through links in an email. Also, be aware of the following tips to help you identify fake web pages:

- Pay attention to the address bar. To be on the safe side, make sure the website starts with https:// before entering any personal information.
- Check the domain name. Make sure that the website that you are on is correctly spelled and not mimicking a well known brand or company.
- Watch for poor grammar and spelling. An excess of spelling, punctuation, capitalization, and grammar mistakes can indicate that the website was put together fairly quickly with no regard for professionalism.
- Look for reliable contact information. If you can find another way to contact the brand or company, reach out to them to confirm the email is real.

Walk away from deals that are too good to be true. Some retailers will discount older merchandise but if the latest item is also heavily discounted, walk away. It's probably too good to be true!