

Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984



Factoring In Multi-Factor Authentication

Multi-factor authentication (MFA) is a simple step that greatly increases cyber security for your business. With MFA, you need a password AND a secondary code from another source to gain access. This is often a code in an app like Google Authenticator or a code sent via text to your phone.

It's included in every Microsoft 365 subscription, but it is a feature that needs to be turned on. Some people don't turn on this option because it's a slight inconvenience. The extra step is inconsequential when compared to the added security features of implementing MFA. Its also required for most cyber liability insurance policies.

Give us a call if you need help implementing multi-factor authentication for your business!

July 2022



This monthly publication provided courtesy of Ryan Haislar, President of Computerease.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"



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 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

Continued on pg.2

Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)

Continued from pg.1

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

“Compliance and cyber security work best when they're aligned, so it's incredibly important that your business has a plan for compliance and cyber security.”

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.

Free Report Download:

The Business Owner's Guide To IT Support Services And Fees

You'll learn:



- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.computer-service.com/ITbuyersguide

Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)

Shiny New Gadget Of The Month:



Airmoto

Imagine you're driving with your family on vacation in the middle of winter. All of a sudden, the road feels much bumpier, so you pull over and get out to check your tires. To your dismay, you discover one of your tires has gone flat. The closest gas station is over a couple of miles away, and your spare can't handle the adverse conditions. So, what should you do? With Airmoto, you never have to worry about this situation.

Airmoto is a rechargeable compact air pump that provides up to 120 psi. In only 10 minutes, you can inflate your car's tires to the proper tire pressure. Airmoto can be used to pump up balls, bike tires and even truck tires. It's practical, not very heavy and quite affordable. Airmoto is the perfect addition to any roadside assistance kit.

The 3 Hardest Questions About Your Career

One of the best parts of my job is helping people strategize about their careers. Success at work plays a large role in how we view the successes in our lives. If someone doesn't feel like they're succeeding or fulfilled at work, they probably don't feel like they're living a very fulfilling life.

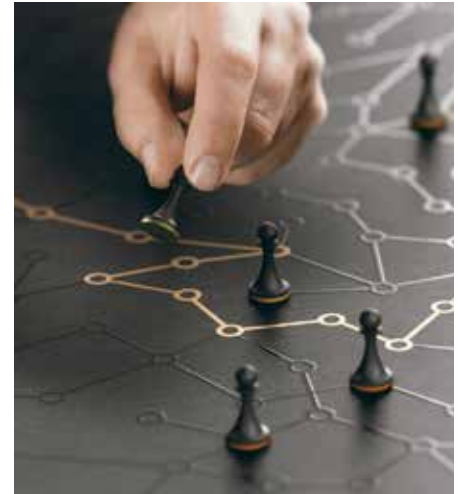
My team and I have advised many people from various backgrounds over the years. From billionaire entrepreneurs who are looking to brainstorm ideas for the next stage of their careers to private equity titans who are solely focused on dealmaking, I've learned that background doesn't always matter. People from nearly every background still have the same challenges when it comes to career management.

Luckily, there are three questions you can ask yourself to help decide the next steps you should take for your career.

First, ask yourself where your skills lie. You also need to gain an understanding of the work that you're willing to do. Once you've found the sweet spot between your skills and what you're willing to do, you're ready for the next step.

You should then ask yourself about potential career paths. It's best to come up with three career paths that you could realistically follow. While one could be a promotion or growing in your role, you should also consider working for other companies or even starting your own business.

The final question you should ask yourself



relates to the people you know. You need to think about 10 people who can help you get your dream job. It's not about putting out a blast message to all of your friends and followers on social media. Instead, you should focus on those who know your work ethic. Start with bosses who know of your work ethic and are well-respected. Any clients or customers who truly appreciate your work should also go on the list as well as well-connected friends and family - and even a recruiter or two. Once you've created a list of 10 people, send them all a message asking for ideas to help you land your dream job. Those brainstorming sessions could easily turn into referrals if done right.

Maybe one day, career management will be automated and our dream opportunities will approach us. But until then, it'll take hard work to reach your goals. If you don't know where to start, try asking yourself these three valuable questions.



Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

■ 3 Types Of Technology Every Business Needs

Over the past 20 years, technology has developed rapidly and advanced to levels that previously only existed within the confines of our imaginations. Whether you're an entrepreneur starting a new business or a seasoned business owner, there are many pieces of technology you can incorporate into your business to produce better results.

Digital marketing tools have seen some of the biggest advancements over the past decade. To stay ahead of the competition, you need to have an informative and useful social media presence that coincides with your website and other digital campaigns. You also need to invest in cloud technology since it will allow your company to revolutionize how you share information. If your business deals with customers, it can be incredibly beneficial to find customer relationship management software that works for you. Various studies have shown a direct correlation

between using CRMs and positive customer retention.

■ 4 Ways Businesses Can Go Green

There's been a renewed focus on how businesses interact with the environment. There are many consumers who prefer to do business with companies that are more eco-friendly. While it's great for attracting new clientele, putting your business on the path to a greener and cleaner future is the best way to stay environmentally conscious. Don't know where to start? Try out these four easy methods for a greener workplace.

- Avoid using paper, and go digital where you can.
- Allow your employees to work remotely whenever possible to help eliminate carbon emissions.
- Analyze your company's current consumption and waste management practices and make adjustments where needed.

- Partner with environmentally conscious vendors and partners so all of your processes will be as green as possible.

■ Be Cautious Of These 3 Cyberthreats

If you own or operate a small business, you're probably aware of some of the different methods that cybercriminals will use to try to steal sensitive information from your business, but there are some new threats making headlines. A recent report from CyberCatch saw the cyber security platform provider review 20,000 randomly selected small businesses in the U.S. for vulnerabilities that can be exploited by cybercriminals. It found that "spoofing," "clickjacking" and "sniffing" are new methods they are exploiting, but what do these terms actually mean?

- **Spoofing** happens when a cybercriminal uses a fake IP address to pretend to be someone who has access to the company's private system.
- **Clickjacking** occurs when a user clicks on something on their computer that appears harmless but is actually malicious.
- **Sniffing** takes place when hackers intercept a network's traffic to access unencrypted data.

It's important to stay up-to-date on all the new methods used by cybercriminals in order to keep your business protected.



"Is that computer, down there, the one you were having problems with?"