# CST Tech News

## What's New

In the last couple of months, I have been bombarded with Cyber Security Insurance Policy renewals for my clients. These policy renewals are tricky and answering them honestly is the difference between successfully honoring a claim. Hopefully, none of us will need to file a claim but insurance is one of those "in case of emergency" situations and we would be stupid and irresponsible not to have it.

As I work on the latest renewal for a client, there are a few items I want to remind all of you about. Some of the items on the renewal are easy to implement and FREE. Others are necessary and may cost but without them, it could put you out of business.

Here are some things ALL of you need to implement NOW:

1. Two factor authentication – this is where your logins require an additional code sent to either email or cell phone to authenticate who you are. This is FREE and a must to protect your accounts.
2. Login credentials for your users to access their computers. Yes, everyone should have to type a password to get into their computer and they should NOT be an admin user. All of you should have an admin account but your employees should not have those

## July 2022

This monthly publication provided courtesy of Shawn & Lisa Brown, Owners

**Our Mission:**

To provide outstanding technology services to our customers allowing them to focus on their business.

# Compliance And Cyber Security

## Why Both Are Important

In the world of business, you'll inevitably hear about the many ways to beef up your cyber security to ensure your company's and clients' safety. However, another term is often heard when discussing cyber security: compliance. It's not talked about as often, but both cyber security and compliance are essential for any business to succeed.

Compliance helps businesses keep consumer information protected, and this compliance is fulfilled when businesses and organizations prove that their cyber security practices meet specific security regulations and standards set by third parties like government agencies. Compliance is not optional; businesses must meet these requirements to protect sensitive information as well as their clients. Failure to meet compliance requirements results in fines, penalties and even legal ramifications.

If your business is compliant with its cyber security protocols, it'll also appear more trustworthy to the clients and other businesses that work with you. One cyber security breach can permanently damage your company's reputation. Customers will no longer want to do business with you for fear that their personal information could become compromised.

While cyber security and compliance sound fairly similar, there is a slight difference between them. Compliance is

*Continued on pg.2*

*Continued from pg.1*

often driven by business needs rather than technical needs, whereas security is driven by the need to protect against constant threats. If you want to maximize your company's cyber security practices, then you'll need to go further.

Overall, compliance and cyber security should work hand in hand. Your initial cyber security plan should be based on compliance. You must know the standard requirements to remain compliant and put the necessary practices in place to achieve that status. This comes down to knowing the exact details of what is necessary to stay protected. You should be specific so your team knows exactly what is needed to protect your business.

You also need to make an effort to document your practices as frequently as possible. You should create a paper trail of everything you have done to stay compliant as well as your added cyber security practices. It can help to add potential

**"Compliance is fulfilled when businesses and organizations prove that their cyber security practices meet specific security regulations and standards set by third parties like government agencies."**

audits and any frequency-bound events to your calendar so you don't get blindsided or miss something important.

After you've gathered all of your evidence and put your cyber security and compliance protocols to work, you can automate many of your reports. That way, you won't have to dig and pull data yourself in the future.

While it might seem like a lot of work to ensure your business remains compliant, companies out there can help. Managed IT services providers, like CST, go above and beyond to ensure your cyber security is bulletproof. While we are taking care of all of your IT needs, we are also ensuring your business remains compliant with any third-party governing bodies. New cyber security threats are introduced every day, and only with strong cyber security and compliance practices can you ensure your business is protected for the foreseeable future.

## Free Report Download:

## Want To Know How To Hire An IT Support Services Company?

## I've written this guide especially for you…


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

**Here's what you'll learn:**

- **The three most common ways IT companies charge for their services and the pros and cons of each approach**
- **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 https://www.cstsupport.com/ITbuyersguide**

credentials. If you are an existing client, we have your Admin account covered but your employees may not have to type a password. If this is the case, please reach out so we can get it corrected.

3. Local, secure backups. Once again, this one is FREE and easy to setup. The problem is that most companies we talk to are using an external hard drive or USB key and keeping it plugged in to their systems. Useless if attacked with virus or ransomware because they will infect that as well. Be sure your backup is regular, and the device is removed and stored in a safe place (either a safe or secured offsite with encryption).

Here are the things that are a must but may cost you:

1. A managed firewall – this is a hardware device that allows us to monitor traffic coming in and out of the web. We have caught so much with our Firewalls and saved our companies thousands of dollars. There is a monthly fee for this, but well worth it considering how it protects you.
2. Email security solutions to include encryption capabilities – if you ever email confidential, PII data, you must have email security with the ability to encrypt information.
3. Offsite cloud-based backup automation. We do this for many of our clients and it is a backup that is off -site and monitored by staff here to ensure it is working and tested.
4. Internal phishing simulations or Security Awareness Training for Staff. Your number one risk for virus and ransomware attacks is your employees. Train them and do it regularly. CST offers quarterly, semi-annual or annual security awareness training and the results are astounding and always informative. You can also educate via staff meetings to ensure your staff know what to do if they get an email that looks suspicious. Problem is it is getting harder and harder to tell.

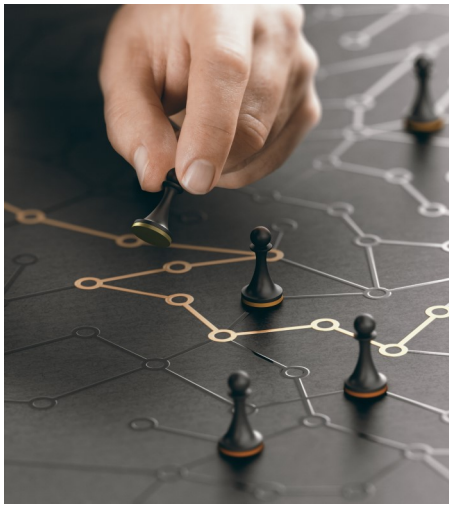
As you can see, there is much to cyber insurance. Answering the questions honestly will determine if your insurance company will cover you for cyber breaches. If you need help, please contact me. I am willing to assist however I can.

Happy 4th of July!

"Passionate not Pushy"

Lisa

# 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 those three valuable questions.

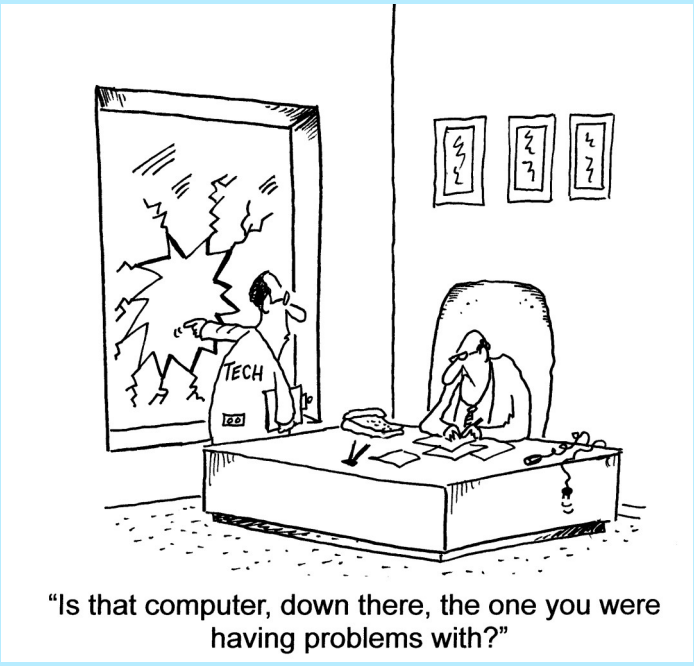
*Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.*

## 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. Educate everyone and reach out if you want to implement some Security Awareness Training.




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

## *It's BBQ Time!*

July 4th tends to be the biggest grilling day of the year and with it being just a few days away, we need all the details!!

What games will you have? Will there be fireworks? What foods will you be serving? Obviously the food is our highest priority.

CST has established lots of traditions and one of them is.....ALL ABOUT THE SNACKS!

You can bet we will be celebrating Independence Day with all the fixings. We, of course, will be closed on Monday July 4th to celebrate the holiday. Snaxville here we come!!!

So whether it is simple burgers and hotdogs or a southern seafood boil let us know. Take a picture of your festivities over the holiday weekend and tag us at *#redwhiteandtech* on our Facebook or Instagram page.

Jessica

## Special Dates

7/4/22
4th Of July

7/15/22
Get To Know Your Customers Day

7/17/22
National Ice Cream Day

7/29/22
Technology Administrator Appreciation Day