The Tech chronicle

Spring, Glorious, Spring!!

Spring -glorious spring! Baseball, Easter egg hunts and festivals all return. Check out the great activities below so you don't miss out on all the fun!

FLASHLIGHT EASTER EGG HUNT
@ Hudson Mills Activity Center – Friday, April 7
Join us for a special, nighttime Easter event. Our trails will be illuminated with colorful lights as older kids enjoy the added challenge of an Easter egg scavenger hunt in the dark. Bring a basket or bag and a flashlight to help search for the eggs in hidden spots along the trail. The scavenger hunt will cover a trail that has an uneven mixed gravel surface with minimal grade changes. Ages: Children ages 8 – 16. Children must be accompanied by a registered adult.

Detroit Tigers Opening Day at Comerica Park
April 6
For many sports fans, the start of Spring means the start of baseball season and the ultimate sports day. April 6th marks Opening Day in Detroit MI, when the Tigers will face off against the Boston Red Sox. Be sure to get your tickets early – the home opener is a favorite among Motor City baseball fans.

Ann Arbor FoolMoon
April 7
FoolMoon is an event in Ann Arbor which celebrates all of the city's passions, including art, performance, and community. Watch a procession of handmade papier-mache luminaries stroll through the Kerrytown, Main Street, and State Street districts. This year's theme is "UFOs" and everyone is invited to participate in the FoolMoon Stroll + Roll.

April 2023

This monthly publication provided courtesy of Dennis Jock of DenBe Computer Consulting.

Did you Know?

The painted turtle is Michigan's state reptile.

What Compliance Standards Does Your Business Need To Maintain?

Understanding HIPAA, NIST And CMMC

Compliance standards are some of the most important things a business needs to maintain to be profitable and well-respected while staying out of legal trouble. Failure to meet these standards will make your business susceptible to fines and legal action. You'll also take a hit on your reputation as customers, vendors and competitors may find your business to be untrustworthy. By enforcing compliance, you're working to promote ethical behavior while protecting the rights of your employees, customers and other stakeholders.

But it's not always obvious which compliance standards apply to your industry or specific business. While most businesses need to ensure they're following Occupational Safety and Health Administration standards for workplace safety, they must also meet Environmental Protection Agency regulations for protecting the environment. There are also compliance requirements that have to do with the information you store and share. Here are three other compliance standards that you should know about if you're a business owner or leader.

Health Insurance Portability And Accountability Act (HIPAA)
You probably already know about HIPAA if you've been to any doctor's appointment in the past two decades. This law was enacted in 1996 to protect the privacy of individuals' personal health information and to ensure the security of that information. HIPAA only applies to "covered entities," which include health care providers, health plans and health care clearinghouses. These entities must comply with the rules set forth by HIPAA when handling protected health information. They must have the necessary administrative, technical and physical safeguards in place to ensure the confidentiality, integrity and availability of the information.

Continued on pg.2

Continued from pg.1

There's been confusion in the past relating to HIPAA, especially during the Covid-19 pandemic. When employers requested vaccination status from their employees, many claimed that this violated HIPAA, which is false. HIPAA only applies to covered entities. It's essential that you know the ins and outs of HIPAA if you work in the health care industry. Noncompliance can lead to fines, legal trouble and, in some cases, the loss of your license to practice medicine.

National Institute Of Standards And Technology (NIST)

The NIST is a nonregulatory agency of the United States Department of Commerce that develops and promotes standards, guidelines and best practices for ensuring the security and privacy of information systems. NIST compliance is vital for any organization that handles sensitive information, such as personal data, financial information or intellectual property. It becomes even more important for heavily regulated industries like health care, finance and government. NIST compliance can help organizations protect against cyberthreats, data breaches and other security incidents. It also helps organizations meet regulatory requirements set by HIPAA.

> **"By enforcing compliance, you're working to promote ethical behavior while protecting the rights of your employees, customers and other stakeholders."**

When you adhere to NIST standards, you'll easily identify vulnerabilities, improve incident response plans and prioritize security measures. The NIST has created a helpful framework and various publications that provide guidelines for various systems and scenarios. If you're looking for a specific publication or are interested in other NIST resources, head to their website, NIST.gov, for more information.

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a framework developed by the U.S. Department of Defense to assess and certify the cyber security practices of organizations that work with the DoD. This framework includes a set of controls and processes that organizations must implement to protect sensitive information and systems from cyberthreats. The CMMC framework applies to all organizations that work with the DoD and handle Controlled Unclassified Information. This often includes defense contractors, suppliers, subcontractors and organizations that provide services to the DoD, such as IT, logistics and engineering. Businesses that support the defense supply chain, including manufacturers, technology firms and professional service providers, also need to adhere to CMMC guidelines. Failure to achieve CMMC certification can result in being unable to bid on or win DoD contracts.

Compliance is something every business needs to be aware of, regardless of industry. Start by investigating HIPAA, NIST, and CMMC to see if their rules and regulations are applicable to your business, then look to other organizations. Doing so will help set your business up for success.

GoDaddy Hacked!

Web hosting giant GoDaddy says it suffered a breach where unknown attackers have stolen source code and installed malware on its servers after breaching its cPanel shared hosting environment in a multi-year attack.

While GoDaddy discovered the security breach following customer reports in early December 2022 that their sites were being used to redirect to random domains, the attackers had access to the company's network for multiple years.

"Based on our investigation, we believe these incidents are part of a multi-year campaign by a sophisticated threat actor group that, among other things, installed malware on our systems and obtained pieces of code related to some services within GoDaddy," the hosting firm said in an SEC filing.

The company says that previous breaches disclosed in November 2021 and March 2020 are also linked to this multi -year campaign.

The November 2021 incident led to a data breach affecting 1.2 million Managed WordPress customers after attackers breached GoDaddy's WordPress hosting environment using a compromised password.

They gained access to the email addresses of all impacted customers, their WordPress Admin passwords, sFTP and database credentials, and SSL private keys of a subset of active clients.

After the March 2020 breach, GoDaddy alerted 28,000 customers that an attacker used their web hosting account credentials in October 2019 to connect to their hosting account via SSH.

GoDaddy is now working with external cybersecurity forensics experts and law enforcement agencies worldwide as part of an ongoing investigation into the root cause of the breach.

Links to attacks targeting other hosting companies

GoDaddy says it also found additional evidence linking the threat actors to a broader campaign targeting other hosting companies worldwide over the years.

"We have evidence, and law enforcement has confirmed, that this incident was carried out by a sophisticated and organized group targeting hosting services like GoDaddy," the hosting company said in a statement.

"According to information we have received, their apparent goal is to infect websites and servers with malware for phishing campaigns, malware distribution and other malicious activities."

GoDaddy is one of the largest domain registrars, and it also provides hosting services to over 20 million customers worldwide. Who is hosting your website? Call DenBe Consulting if you have concerns.

Impress Any CEO In 3 Easy Steps

You have a meeting scheduled with a CEO. Your goal is to convince them to either spend $1 million on your product or service, hire you or invest in your idea. What's your strategy?

Many people "show up and throw up" and push a lot of information at the CEO, either verbally or by PowerPoint. A CEO will not hire you simply because you show that you know what you're talking about. Another flawed approach is to phrase your request as a "we ought to." CEOs don't decide to do things just because other people say they should do something. Worse yet is when people only talk about why they want something to happen, ignoring the CEO's wishes, concerns and perspective.

So, how do you successfully convince a CEO?

1. **Seek first to understand the CEO's perspective.** That is Stephen Covey's advice. It needs no further explanation. Your first step in discussing a topic with a CEO is to put all your energy into asking probing questions, listening and learning what the CEO thinks about a topic and why. Forget about your agenda or your needs for a moment.

2. **Reflect the CEO's perspective to their satisfaction.** This step is tricky. Most people cannot objectively reflect or restate another person's perspective about a topic without putting their own slant on it. I first learned this step during my psychology Ph.D. training during a class on conflict resolution. At this step, you must restate the CEO's perspective on the topic, simply and without putting words in their mouth or trying to spin it in your favor. You know you have succeeded once the CEO says the magic word, "exactly." This means that the CEO believes you understand their perspective. Then, and only then, have you earned permission to move to the final step.

3. **Propose your idea as a way to help the CEO achieve their goals.** The mindset for this step is not that you are about to trick or fool a CEO into doing something that's not good for them. Your mindset is that you are about to convince a CEO to do something that *is* good for them. (And by the way, if what you are about to propose is not in the CEO's best interests, then don't propose it!) A simple way to present your idea is to say, "Your goals are X, your concerns are Y, so I propose you do Z."

Contrary to popular belief, great ideas don't sell themselves. It takes a skillful leader to successfully convince a CEO, and now you have the tools to do so.

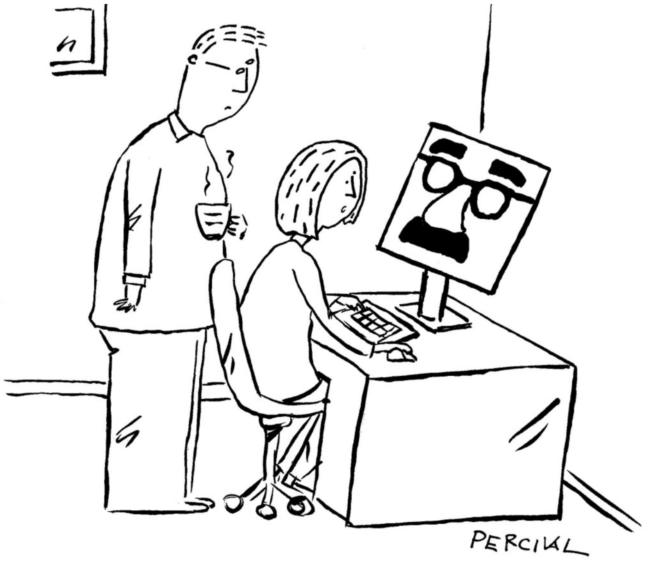
Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *bestsellers. He stays active in his community and has advised many government officials.*

Are You Addicted To Work? 2 Ways To Help Take Your Life Back

Many business owners and entrepreneurs will dedicate their entire lives to their businesses to ensure success. They'll regularly work 60- to 80-hour workweeks, sacrificing their free time to focus on their business. In many ways, it's an addiction that can be incredibly damaging to an individual's mental health. Recent studies have shown that those who work too much are more susceptible to burnout, chronic stress and strained relationships. If you find yourself spending too much time in your business, there are a few things you can do to fight your work addiction.

Reassess Your Goals.
Why are you working so hard? What do you want to achieve? Is it actually possible, or are you working yourself into the ground for an unobtainable dream? These are questions you need to ask yourself if you feel you're working too much. Reflect on your goals and determine if they're still what you want for yourself and the business. If not, or if your goals are not feasible, it's time to readjust and create new ones.

Trim Your Task List.
Working too long every day usually stems from trying to accomplish too much daily. Take a step back and think about what you can truly accomplish in 8–10 hours. Don't put too much on your plate because you'll feel like you need to complete everything before you head home. Delegate the less important tasks if you have a team supporting you. You don't have to do everything in one day on your own.



"The computer's acting funny."

Why Aren't My Employees Reading My E-mails?

How often do you send out e-mails to your employees? Have you ever talked with an employee about prior communication you sent, but they tripped their way through the conversation? It happens all the time across various industries. Employees don't always read communications from upper management, and you're left trying to figure out why. Sure, you could blame it on the employees just not wanting to read, but there's often a deeper issue involved. Here are a few reasons your employees are ignoring your e-mails.

- **Improper Timing:** Your employees are less likely to read your e-mails if you send them out at the end of the day.

- **Information Overload:** E-mails with too much information cause your employees to take too much time from their other tasks. Only put the information that's absolutely necessary in your e-mails.

- **Unclear Expectations**: Are your employees required to read your e-mails? They might just ignore the e-mails if they don't think they pertain to their job or provide relevant information.