DTS DanTech Services
Computers under control!™

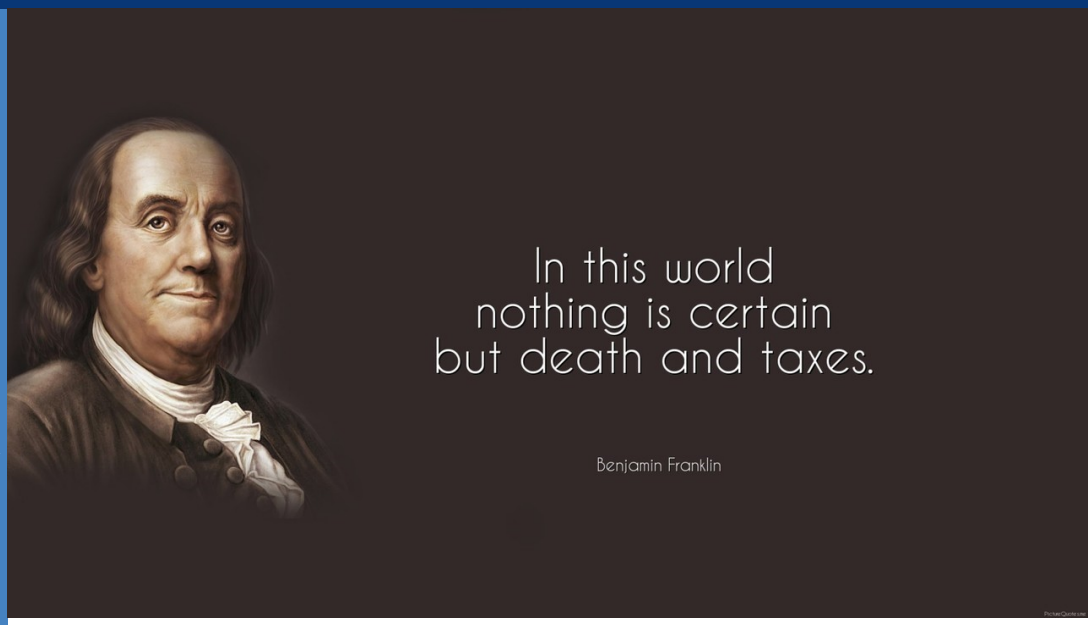
Technology Times April 2024 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "


## What's Inside:



***Got IT Problem? - Click Here!***




# Death & Taxes (and Compliance)

If you've seen the movie, "Meet Joe Black", you're familiar with how Death, in the guise of Joe Black, picks up on the term "Death & Taxes" as the two things in life that are unavoidable. This phrase is often considered a truth to our lives and I'm not here to disagree with it. I will say that after attending a conference on Cyber Security that revolves around upcoming requirements for contractors, subcontractors, and service providers that work with DoD (Department of Defense), we can now add Compliance. Death, taxes, and compliance.

Working under any contract that includes the DoD, compliance to certain specific standards has been in place under DFARS (Defense Federal Acquisition Regulation Supplement) rules, yet changes in this structure are rapidly approaching. These changes surrounding CUI (Controlled Unclassified Information) will ramp up requirements significantly.

Although the roll out time will have an impact on slowing the burden, starting in 2025 these contracts will reference requirements that must be met for cyber security purposes. This is not an easy task.

Why do I mention this? Many of our clients don't venture into this space and may not have any immediate compliance standards, like HIPAA or PCI, that are considered as part of their business model. That too is not my point. HIPAA & PCI have been around for decades, you say. Yes, they have.

Step back a moment. Did your last E&O or liability insurance renewal have questions about cyber security? I'd be surprised if it didn't. This was not so 5 years ago, in many cases. If questions were asked, it was usually a short list of generally innocuous questions. Step forward a moment: are you asked more questions about your cyber security posture now?

*- Continued on page 4*

## GPT-5 might arrive this summer as a "materially better" update to ChatGPT

When OpenAI launched its GPT-4 AI model a year ago, it created a wave of immense hype and existential panic from its ability to imitate human communication and composition. Since then, the biggest question in AI has remained the same: When is GPT-5 coming out? During interviews and media appearances around the world, OpenAI CEO Sam Altman frequently gets asked this question, and he usually gives a coy or evasive answer, sometimes coupled with promises of amazing things to come.

According to a new report from Business Insider, OpenAI is expected to release GPT-5, an improved version of the AI language model that powers ChatGPT, sometime in mid-2024—and likely during the summer. Two anonymous sources familiar with the company have revealed that some enterprise customers have recently received demos of GPT-5 and related enhancements to ChatGPT.

One CEO who recently saw a version of GPT-5 described it as "really good" and "materially better," with OpenAI demonstrating the new model using use cases and data unique to his company. The CEO also hinted at other unreleased capabilities of the model, such as the ability to launch AI agents being developed by OpenAI to perform tasks automatically.

We asked OpenAI representatives about GPT-5's release date and the Business Insider report. They responded that they had no particular comment, but they included a snippet of a transcript from Altman's recent appearance on the Lex Fridman podcast.

Lex Fridman(01:06:13) So when is GPT-5 coming out again?
Sam Altman(01:06:15) I don't know. That's the honest answer.
Lex Fridman(01:06:18) Oh, that's the honest answer. Blink twice if it's this year.
Sam Altman(01:06:30) We will release an amazing new model this year. I don't know what we'll call it.

*- Continued on page 3*

## College wisdom to the rescue! Helping local businesses improve their cybersecurity defenses

A lot of small business owners are concerned about cybersecurity; they don't know what they can do to ensure their networks are safe.

Small businesses -- including non profits, local public services, and mom-and-pop companies --often don't have the resources to put up much of a defense in their cybersecurity. But thanks to a new initiative, many colleges and universities are setting up free clinics to assist local businesses with their cybersecurity needs.

Teams of college IT students, who are actively training, researching, and studying cybersecurity prevention, are also advising executives on what's most important in network safety, such as password safekeeping and phishing scam recognition.

More than 15 schools are offering these clinics as a part of the Consortium of Cybersecurity Clinics. Participants include Louisiana State University (LSU), Indiana University (IU), and Massachusetts Institute of Technology (MIT), among others.

The free services provided through these clinics include cybersecurity risk assessments, creating incident response plans, and helping to establish Multi-Factor Authentication, as well as consultation and training.

Students in cybersecurity fields can spend a semester working at their school's cybersecurity clinic for course credits. They will choose from three specialties: Threat and vulnerability assessment, cyber risk assessment, and cyber defense. Each student can help three clients a semester.

Small business owners who have worked with these clinics appreciate that students work individually with them, getting to know the business as well as their specific cybersecurity needs and weaknesses, advising them accordingly. Many clients compliment them for explaining complicated processes in layman's terms. One clinic had the chance to work with a local fire department to create a plan to prepare employees if their systems go down as the result of a cyberattack.

The main goal of cybersecurity clinics is to ensure that local businesses can protect their most valuable assets. They also play a significant role in helping the local economy. By providing free cyber security assistance, these clinics are helping small business free up resources to allocate elsewhere, thus running more efficiently.

Similar to clinics in which law and medical students provide pro-bono services, these clinics help information security students enrich their education and develop specific skills through real world problem solving, gaining exposure to different areas of cybersecurity.

These university cybersecurity clinics work with about four to seven clients at a time, and the service needs vary, from preventing ransomware attacks to crafting incident-response plans. There is already a waiting list at many universities for businesses requesting services from cybersecurity clinics.

## Shiny App Of The Month


### How to fly the friendly skies of Google Earth

Many Google Earth users don't realize it offers a virtual flight experience that allows you to traverse the world from the comfort of your own home. You must have Google Earth or Google Earth Pro installed on your computer. It will not work with the online version of Google Earth.

**Go to Tools >** Enter Flight Simulator. (Or use Ctrl + Alt +A on Windows; or Command + Option + A on Mac)

**Choose your aircraft.** The options Google offer: Cirrus SR22 (recommended for beginners) or F16 Fighting Falcon (recommended for skilled pilots). To change planes, you must exit the flight simulator first.

**Select your starting location.** You can pick an airport from a given list or choose to start from your current location. Another option is to start from where you ended your last flight simulator session.

**Heads-up Display:** While you're flying, you can monitor everything you need on the display that shows on the screen, including an air speed Indicator, altimeter, heading indicator, and many other gauges relating to throttle, rudder, aileron, elevator, pitch, altitude, and more.

To access the flight simulator on Google Earth 4.2:

**Go to the Fly** to box in the upper left corner.

**Type Lilienthal** to open Flight Simulator. If you're directed to Lilenthal, Germany, it means you've already launched Flight Simulator. In that case, you can open it from Tools > Enter Flight Simulator.

- "GPT Chat 5 may arrive this summer " - Continued from page 2

Lex Fridman(01:06:36) So that goes to the question of, what's the way we release this thing?
Sam Altman(01:06:41) We'll release in the coming months many different things. I think that'd be very cool. I think before we talk about a GPT-5-like model called that, or not called that, or a little bit worse or a little bit better than what you'd expect from a GPT-5, I think we have a lot of other important things to release first.

In this conversation, Altman seems to imply that the company is prepared to launch a major AI model this year, but whether it will be called "GPT-5" or be considered a major upgrade to GPT-4 Turbo (or perhaps an incremental update like GPT-4.5) is up in the air. Like its predecessor, GPT-5 (or whatever it will be called) is expected to be a multimodal large language model (LLM) that can accept text or encoded visual input (called a "prompt"). And like GPT-4, GPT-5 will be a next-token prediction model, which means that it will output its best estimate of the most likely next token (a fragment of a word) in a sequence, which allows for tasks such as completing a sentence or writing code. When configured in a specific way, GPT models can power conversational chatbot applications like ChatGPT.

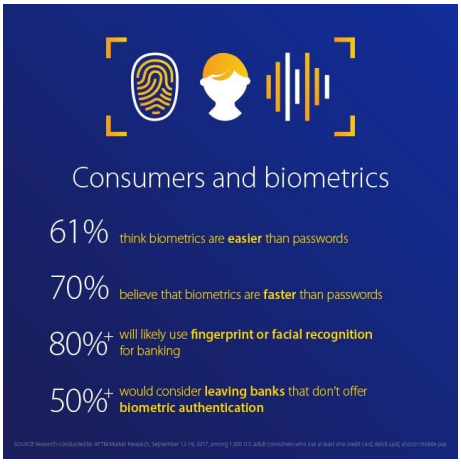
OpenAI launched GPT-4 in March 2023 as an upgrade to its most major predecessor, GPT-3, which emerged in 2020 (with GPT-3.5 arriving in late 2022). Last November, OpenAI released GPT-4 Turbo, which lowered inference (running) costs of OpenAI's best AI model dramatically but has been plagued with accusations of "laziness" where the model sometimes refuses to answer prompts or complete coding projects as requested. OpenAI has attempted to fix the laziness issue several times.

LLMs like those developed by OpenAI are trained on massive datasets scraped from the Internet and licensed from media companies, enabling them to respond to user prompts in a human-like manner. However, the quality of the information provided by the model can vary depending on the training data used, and also based on the model's tendency to confabulate information. If GPT-5 can improve generalization (its ability to perform novel tasks) while also reducing what are commonly called "hallucinations" in the industry, it will likely represent a notable advancement for the firm. According to the report, OpenAI is still training GPT-5, and after that is complete, the model will undergo internal safety testing and further "red teaming" to identify and address any issues before its public release. The release date could be delayed depending on the duration of the safety testing process.



Of course, the sources in the report could be mistaken, and GPT-5 could launch later for reasons aside from testing. So, consider this a strong rumor, but this is the first time we've seen a potential release date for GPT-5 from a reputable source. Also, we now know that GPT-5 is reportedly complete enough to undergo testing, which means its major training run is likely complete. Further refinements will likely follow.

## Biometrics vs. Passwords




Biometrics -- such as fingerprint, voice, or facial recognition -- when used to permit entry or access to a device or location, is technically safer than a password because it's harder for cyber-criminals to replicate, compromise, or steal. Also, Biometric authentication is quicker and more convenient than typing passwords. Users don't need to remember complex sequences or worry about resetting them if they're forgotten.

These benefits, though, come with some hefty drawbacks. For one thing, in the case that your biometric info is hacked, it cannot be changed like a password; it remains compromised forever. Then there's the privacy concern. Employees, for instance, may not be comfortable knowing that executives in their companies have access to, and can even share, their personal data.

And for the employers, there's the costliness of implementing biometric authentication. Devices, such as fingerprint scanners and facial recognition cameras, require an investment of money, time, and maintenance.

While biometric authentication offers improved security and convenience, it also comes with challenges related to privacy, accuracy, and implementation. Combining biometrics with passwords can provide a robust authentication solution.

*- "Death & Taxes (and Compliance) " - Continued from page 1*

In short, compliance is coming to an industry near you. It may not (yet) be mandated by the federal, state, or local governments, yet it's happening through insurance companies that rely on the data you provide as a business for your coverage. The data that says that your business has policies and procedures in place. The form that has been signed that can hold your company liable for misstatements.

"But I just work for them!" Given the audience that reads our newsletters, that's likely the case. I'll note that your paycheck relies on the ability of your employer to operate. To generate income. To pay vendors. And employees.

We are all in this together. Every one of us. At the management level, having the written policies in place is crucial. Without written policies, insurance companies can mark you non-compliant. At the user level, being the steward of your own security is equally important. Using MFA wherever possible, setting strong passwords, not installing apps that are unknown to your IT department, knowing whether you're dealing with a valid email. Having taken the expected user awareness training. All of which are simple brushstrokes of what's required. This is also information, knowledge, and awareness that can be taken home for use in your personal life to protect your personal accounts.

It's not always convenient. We can all agree on that. Step back again, this time to look at the larger picture. Whether a job provider or a job holder, compliance requirements are affecting all of us—whether we choose to admit it or not. I suggest that we choose to admit it and to cooperate in working towards it.

**Do your own research. Or you're welcome to use some of mine (courtesy of Copilot):**

*Statistics related to cybersecurity insurance, including income and payouts for cyber security claims:*

### Global Cybersecurity Insurance Market:

- In 2021, the global market for cybersecurity insurance was valued at **USD 7.60 billion** and is projected to reach **USD 20.43 billion** by 2027[1].
- The US market alone accounted for **$2.38 billion** in 2020[1].

**Claim Payouts and Exclusions**:

- Over the past three years, cyber insurance claims have surged by **100%**, with payouts increas-ing by a total of **200%**. The peak number of claims occurred in **2021**, reaching **8,100**[1].
- Interestingly, **99%** of all cybersecurity insurance claims originated from **small and medium-sized enterprises (SMEs)** with annual revenue under **$2 billion**[1].
- The average claim cost for an SME due to a ransomware event is **$485,000**, while the overall average claim across all organizations stands at **$812,360**[1].

**Market Growth**:

- The global cyber insurance market is expected to grow at a compound annual growth rate (CAGR) of **24%**, reaching **USD 20.43 billion** by 2027[1].
- The US market remains the largest contributor to the cyber insurance industry, and it is predict-ed to continue driving growth and adoption over the next six years[1].

**Profitability for Insurance Companies**:

- Cyber insurance policies tend to be **profitable** for insurance companies. The **loss ratio**, calculat-ed as the ratio of claims paid out to premiums received, indicates this profitability[2].
- Insurers may introduce specific terms, such as limiting reimbursement for extortion payments or adjusting coverage, to maintain profitability[3].

In summary, the cyber insurance landscape is evolving rapidly, with increasing claims and a focus on SMEs. Organizations must carefully assess their coverage needs to navigate the complex world of cybersecurity risks and insurance[1].