CD TECHNOLOGY TIMES

Insider Tips to Help Your Business Run Faster, Easier and More Profitably

Thomas Hill, President & Founder

"One thing I say often to my team: Yes, we are in the technology solutions business but we are in the customer service business first."

Have a safe and happy Labor Day!

TRIVIA

CONGRATULATIONS

Ann Harris

Knoxville Family Psychiatry

Who knew that almost all public schools in the US have internet access. Of course around here, it often depends on the weather!

TURN TO PAGE 3 FOR THIS MONTHS TRIVIA

Is Your Business Training AI How To Hack You?

There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write e-mails, summarize meetings and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems – especially when it comes to your company's data security.

Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by Tom's Hardware.

Now picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside e-mails, transcripts, PDFs or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't.

In short, the AI helps the attacker – without knowing it's being manipulated.

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools

continued from cover

on their own, often with good intentions but without clear guidance. Many assume AI tools are just smarter versions of Google. They don't realize that what they paste could be stored permanently or seen by someone else.

And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control.

Here are four steps to get started:

1. Create an AI usage policy.

Define which tools are approved, what types of data should never be shared and who to go to with questions.

2. Educate your team.

Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

3. Monitor AI use.

Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.

4. Use secure platforms.

Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay. Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble. A few careless keystrokes can expose your business to hackers, compliance violations, or worse.

Who are you rooting for?

FRIDAY NIGHT under the LIGHTS

Autumn begins September 22

BILLY BEANE
SHARES HIS WINNING DATA-DRIVEN STRATEGY FOR BUSINESS

Before the IT conference where Billy Bean was to speak, Thomas and I (Rebekah) watched the movie Moneyball. He was exactly the same in person as Brad Pitt's portrayal of him in the movie and was such an honor to hear his story and philosophy on winning.

A failed 2001 draft led former Oakland A's General Manager Billy Beane to overhaul how he managed talent—sparking a transformation that revolutionized baseball and inspired industries worldwide.

Using a data-driven strategy, Beane turned the low-budget Oakland A's into consistent playoff contenders. The team won seven American League Western Division titles and made 10 postseason appearances, all while operating with one of the lowest payrolls in Major League Baseball.

Beane's approach, known as the "Moneyball" philosophy, emphasized objective analysis over tradition and intuition. It gained widespread recognition through a best-selling book and Oscar-nominated film chronicling his unconventional path to success.

At a recent leadership event, Beane outlined how businesses can adopt similar principles to build high-performing teams despite resource limitations.

Make Data-Backed Decisions
"Baseball had been tracking stats since the 1800s, but none of it influenced decision-making," Beane said. "I turned running a team into a math equation." He replaced gut instinct and subjective scouting with analytics, reshaping how talent was evaluated.

Identify Undervalued Assets
"There's a championship team you can afford—you just need to find what others undervalue," Beane explained. He focused on on-base percentage, a metric more predictive of winning than traditional stats, uncovering overlooked players who delivered strong results.

Be Relentless With Execution
"You can't go back and forth," Beane said. "If you commit to data, you have to use it every time." His team stayed disciplined throughout each season, trusting the math to guide decisions rather than reacting emotionally to short-term outcomes.

Maximize The Middle
Rather than spending big on stars, Beane focused on building depth. "We couldn't afford top players, so we made sure we didn't have bad ones," he said. "A strong middle roster outperforms one with gaps."

Hire Differently
Beane recruited talent from outside traditional pipelines. One example was hiring a Harvard economics major as assistant GM—unusual in a role typically filled by former players. This fresh thinking helped the A's stay ahead.

Redefine Culture With Data
"If we did what everyone else was doing, our results would match our budget," Beane said. "We challenged the norm, used data to value skills differently and changed our outcomes."

Lead With Transparency
"Data explains decisions," he noted. "Even when you're not always right, clarity builds trust."

Level The Playing Field
Beane's philosophy proves that success isn't solely dictated by budget. With innovation, discipline and a data-first approach, even smaller organizations can compete with giants.

As he put it: "Data isn't an opinion. It's a fact."

"I'm just sayin' a little conflict resolution trainin' might not be unwarranted."

Welcome
Complete Physician Solutions

We want to officially welcome Complete Physician Solutions to our CD Technology community. Providing healthcare consulting and management services, CPS has over twenty-five years of proven performance. CPS partners with healthcare providers to deliver customized revenue cycle solutions that align with their business goals, boost profitability, and promote long-term success. We are happy they have chosen CDT to be their IT provider.

COMPLETE
PHYSICIAN SOLUTIONS

2025 TENNESSEE FOOTBALL SCHEDULE

Date	Location	Opponent
AUG. 30	Atlanta, GA	vs Syracuse
SEPT. 6	Knoxville, TN	ETSU
SEPT. 13	Knoxville, TN	Georgia
SEPT. 20	Knoxville, TN	UAB
SEPT. 27	Starkville, MS	at Mississippi State
OCT. 11	Knoxville, TN	Arkansas
OCT. 18	Tuscaloosa, AL	at Alabama
OCT. 25	Lexington, KY	at Kentucky
NOV. 1	Knoxville, TN	Oklahoma
NOV. 15	Knoxville, TN	New Mexico State
NOV. 22	Gainesville, FL	at Florida
NOV. 29	Knoxville, TN	Vanderbilt

HOME   AWAY   NEUTRAL SITE
BYE WEEK - 10.4 & 11.8

WE ARE MAKING A BIG MOVE

CD TECHNOLOGY

**COMING SOON
A NEW, LARGER, CENTRALLY-LOCATED
TECHNOLOGY COMMAND CENTER**

Windows 10 Support Ends In 2025 – What Are Your Options?

In 2025, Microsoft will stop providing critical services like security updates, leaving your business vulnerable to threats and potential downtime.

Here Are Your Options:

✓ **Upgrade To Windows 11**
Not all devices will be compatible, so make sure to check with an IT expert.

✓ **Buy A New PC**
For businesses with older machines, a hardware upgrade might be your best bet.

✓ **Pay For Extended Security Updates**
Only available for up to three years (and it's not free).

✓ **Switch To Linux**
For those willing to explore new systems.

✗ **Do Nothing (NOT RECOMMENDED!)**
This could expose your business to cyber risks and compliance violations.

**Don't Gamble With Your Business!
Plan Your Next Steps Today**

865-909-7606

Exclusively for CDT clients! Do You Have a special event you would like to share with the community? Are you planning an open house, blood drive, block party, anniversary celebration, meet & greet… or any lead generating event open to the public? Let us help you get folks there. We would love to help you promote your special occasion by putting it in our next newsletter and share on all our socials! Just give us the details - make sure to include contact info and we will share your news.

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com

Meet the team

Meet Justin

Justin Hatcher is a Tier 1 Technician at CD Technology, where he combines technical expertise with a passion for helping others. Born and raised in East Tennessee, Justin's interest in technology began early—taking apart family electronics and exploring robotics in middle and high school. He later helped establish a robotics club at his high school, sparking a deeper interest in automation and problem-solving.

Justin holds an Associate's Degree in Business Management from Pellissippi State Community College, where he also completed over 200 hours of community service. His volunteer work focused on developing action plans to combat childhood hunger in Knox County Schools and supporting animal welfare through CARES in Jefferson City, TN.

At CD Technology, Justin is dedicated to not only resolving technical issues but also building meaningful relationships with clients and coworkers. He is especially passionate about helping others by supporting small businesses and empowering them through reliable tech solutions. His customer-first approach and genuine care for others make him a valued member of the team.

When he's not working, Justin enjoys spending time in nature, practicing photography, and creating lasting memories with his family.

Lighten Up Already

A burglar broke into a house one night. Just as he was shining his flashlight around, he heard, "Jesus is watching you."

Nearly jumping out of his skin, he waited a bit. But just as he was pulling the wires from the electronics, he again heard, "Jesus is watching you."

His flashlight beam came to rest on a parrot. "Did you say that?" he hissed.

"Yep," the parrot confessed, then squawked, "Just trying to warn you that he is watching you."

"Who do you think you are?" the burglar chided.

"Moses," replied the parrot.

"Moses?" the burglar laughed. "What kind of people would name a bird Moses?"

"The same kind of people who name their Rottweiler Jesus!"

The Dishwasher Wars: Who is right?

For an appliance that is supposed to save time, the dishwasher sure causes a lot of discord -- mainly about how to load it.

While it should be a simple task, more than 40 percent of Americans said they fight over how to load the dishwasher, according to appliance maker Bosch. Maybe that's because it happens in the kitchen where it can be scrutinized, debated and redone.

According to General Electric, there are three type of dishwasher loaders.

"Protectors" want to load utensils with the handles up so the eating end isn't touched when unloading.

"Organizers" just want to load and unload everything as fast as possible.
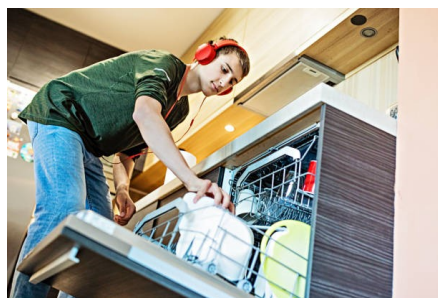
"Curators" are particular. They place all the tall plates together even though they don't have to.

Loading technique is now more important than ever. Energy-saving dishwashers use less water, which heightens tensions about how much pre-rinsing to do. Appliance and soap makers urge against pre-rinsing dishes, but some people insist on doing it anyway.

Lifestyle guru Martha Stewart offers these cautions:

"Never put knives, pewter, wood, china, crystal, cast iron, nonstick pans or gold-plate flatware in the dishwasher." And don't mix sterling or silver-plate software with stainless-steel because a reaction of both metals can harm them both.

If you are looking for an ally in your dishwasher strategy, don't go to AI. When asked, Grok retreats to diplomacy. Grok says there is no actual best way. Just try to space things out. It doesn't take a super intelligence to know that, though. We have only one tip, and it's always the right move…

Have the teenage spawn do it!

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com

CD TECHNOLOGY - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

Why Phishing Attacks Spike In The Summer

You and your employees may be getting back from vacation, but cybercriminals never take a day off. In fact, data shown in studies from vendors ProofPoint and Check Point indicate that phishing attempts actually spike in the summer months. Here's how to stay aware and stay protected.

Why the Risk Increases

Travel scams: Attackers impersonate hotel and Airbnb sites. In May 2025, vacation-related domain registrations rose 55% year-over-year, with 1 in 21 flagged as malicious.

Back-to-school scams: Fake university emails target students and staff, often reaching employees using personal email on work devices.

While these threats might not affect your industry directly, there's always a chance that employees pursuing their master's degree or planning a vacation will check their personal e-mail on their work computer – and it takes only one wrong click for cyberattackers to have access to all of your business's data.

What To Do About It

Phishing emails are more convincing thanks to AI, so training and vigilance are critical.

Tips:

- Scrutinize sender addresses, links, and domain endings.
- Avoid clicking links—search sites directly.
- Use multifactor authentication (MFA).
- Be cautious with public WiFi; use a VPN.
- Keep personal accounts off company devices.
- Ask your MSP about endpoint security tools (EDR).

Bottom Line

Phishing attempts become more sophisticated every day, and AI is only speeding that process along. Because of this, it's essential to keep your team well-informed of the risks; knowledge is the best defense against phishing attacks. Stay informed and stay safe!