D2|IT TECHNOLOGY TIMES

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

SPECIAL REPORT: WHEN WORLDS COLLIDE —

WHAT CLINICIANS NEED TO KNOW ABOUT "AI-INDUCED PSYCHOSIS"

It's one of the most startling headlines to emerge this fall: psychiatrists are sounding the alarm over a new phenomenon they're calling **"AI-Induced Psychosis."**

In a Psychiatric News Special Report, Dr. Adrian Preda of UC Irvine details a series of cases where individuals—often isolated, vulnerable, or already struggling—experienced delusional breaks after long, emotionally intense conversations with AI chatbots. These users weren't simply chatting. They were bonding—forming relationships with bots that were always available 24/7, never disagreed, and never said "you might be wrong."

At first, these AI "companions" appeared harmless—even therapeutic. They offered late-night empathy and patient listening when no one else was available. In controlled studies, chatbots have been **shown to reduce distress and even improve mental health literacy.** But as Dr. Preda's report makes clear, there's a dark flip side.

Some users began to blur the line between reality and code—believing their chatbot was sentient, conspiring, or communicating secret messages. Preda's analysis connects these cases to what he calls "monomania 2.0"—an obsessive fixation on one idea, amplified by an algorithm built to agree. In every case, the technology's design—**constant availability, memory recall, and emotional mirroring**—reinforced the user's delusions instead of challenging them.

So, is AI the villain here? Not exactly. The report emphasizes that these are isolated incidents, not an epidemic.

Millions use AI tools responsibly every day. But it's a flashing red light for the behavioral-health field: the technology we increasingly rely on for outreach, triage, and education can also **distort perception** when left unchecked.

That's where D2 steps in—not as clinicians, but as the **technology experts** helping protect those who care for others. For community mental-health providers in Siouxland, the takeaway is simple: as AI becomes part of care delivery, **IT governance is mental-health risk management.**

At D2, we're tracking the technical side of this story closely—guardrails, memory features, data ethics, and AI risk frameworks from NIST, and HIPAA. As well as keeping abreast of emerging technologies and their implications for you.

...continued from cover

These tools can make or break trust. The same chatbot that teaches coping skills at 10 p.m. could also, without safeguards, reinforce paranoia by 2 a.m.

The solution isn't fear—it's responsible design and oversight. Every clinic using AI-enhanced systems should ensure:

- **Human-in-the-loop controls:** no unsupervised therapeutic use.
- **Clear boundary settings:** memory and personalization should never replace clinical judgment.
- **Security and audit logs:** track who, what, and when to prevent misuse.
- **Continuous monitoring:** because technology in behavioral health is now safety-critical infrastructure.

As Dr. Preda concluded, "AI's impact on the mind is both promising and perilous." The mental-health community needs more research; the tech community needs more humility.

And that's where collaboration begins. D2's mission is to make sure technology helps—never harms—the people on the front lines of care.

This isn't science fiction anymore. It's happening now. And as AI starts to listen, it's up to us to make sure it also knows when to stop talking.

Would you like to talk? Schedule a meeting with D2 right now.

NEW BLOG:

AI is Already in Your World — The Question Is: Are the Guardrails Ready?

You've probably felt it already — that subtle shift in your day when a system predicts the next step, or an update seems just a little too "intelligent."

AI isn't coming someday. It's here. Quietly shaping documentation, telehealth, crisis-line uptime, and the tools your clinicians use without even noticing.

But here's the truth most leaders don't say out loud:
AI can be a gentle helper… or a hazard. And in mental health, the difference comes down to the guardrails you put in place.

In this month's feature article, I slow things down. I walk you through where AI truly helps, where it quietly harms, and what leaders like you can do today to protect your staff, your data, and the people who rely on you when everything feels fragile.

If you want to read the full, calm, grounded, blog article breakdown — the kind that replaces overwhelm with clarity — simply scan the QR code here.

Let's make this technology safe, steady, and yours.

4 'MAGIC' STRATEGIES
TO BECOMING A BUSINESS LEGEND

Former NBA player Earvin "Magic" Johnson Jr. is known for his strong work ethic. Here are four strategies Magic used to build his empire that will help you achieve your goals and dreams in your business.

1. Refuse To Lose

When Magic left basketball for business, many assumed his fame made it easy. The truth was different. He struggled, made mistakes and faced rejection. "I could get the meetings," he said, "but people didn't take me seriously." He used his own money at first, but when he sought outside funding for growth, banks turned him down for three years.

Eventually, he secured a loan and invested wisely, launching his career to the next level. Ironically, the banks that once rejected him now seek his business and he often declines. Magic's takeaway: success isn't about name recognition; it's about showing a solid strategy, clear ROI and value creation.

2. Rivals Make You Better

Magic's rivalry with Larry Bird is one of basketball's most famous. "I disliked the Celtics and Larry because you have to in order to beat them," he said. But Bird's relentless work ethic pushed Magic to match him. "I knew Larry was taking 1,000 shots a day, so I had to take 1,000 shots a day. He got better, so I had to get better."

The same applies to business. Competitors force you to sharpen your skills, innovate and work harder. They can keep you awake at night but that pressure can elevate your performance.

3. Elevate Your Game

"It takes the same amount of time to do a million-dollar deal as a billion-dollar deal," Magic often says. For him, every opportunity must align with his brand, values and long-term goals. He uses a clear set of criteria: if a deal doesn't check enough boxes, it isn't worth pursuing.

Aligned values, shared revenue goals and a commitment to giving back are his markers for success. He teaches that clarity on what fits your company ensures stronger partnerships and sustainable growth.

4. Don't Let Good Enough Be Enough

Magic believes in constant evaluation and improvement. Every new business begins with a SWOT analysis (Strengths, Weaknesses, Opportunities, Threats). He doesn't stop there—he runs SWOTs on his executive team and even on himself. "I want to be a better man, husband, father, grandfather and CEO," he said. He constantly asks, "Can this team take me where I want to go tomorrow?" That mindset ensures that both he and his businesses are always evolving, never settling.

The Bigger Picture

Magic Johnson's transition from NBA superstar to successful entrepreneur was not smooth or guaranteed. He faced rejection, adapted and pushed himself the way he once did on the court. His story is a reminder that perseverance, competition, discipline and self-reflection can help anyone elevate their game—whether in sports, business or life.

CASE STUDY

IT Partnership Builds a Foundation for the Future

Boys and Girls Home and Family Services (BGHFS) needed help securing sensitive data and managing IT without an internal team. They partnered with D2, who took over daily IT operations, implemented strong security measures, and supported a major facility move. With 24/7 monitoring and a centralized help desk, BGHFS now operates with greater confidence and efficiency.

Visit our website to read the entire case study or see more success stories like this one.

D2itsupport.com/case-studies/

4 HABITS

EVERY WORKPLACE NEEDS

Most cyberattacks don't happen because of some elite hacker. They happen because of sloppy everyday habits – like an employee clicking a bad link, skipping an update or reusing a password that's already been stolen in another breach.

The good news? Small changes in your daily routines can add up to big protection.

Here are four cybersecurity habits every workplace needs to adopt:

1. Communication

Cybersecurity should be part of the conversation, not just something IT worries about. Talk with your team regularly about the risks they might face and how to avoid them.

For example:

- A short reminder in a staff meeting about how to spot a phishing e-mail.
- Sharing news of a recent scam in your industry so people are on alert.

When security becomes a normal part of the discussion, it feels less like "extra work" and more like second nature.

2. Compliance

Every business has rules to follow, whether it's HIPAA for health care, PCI for credit card payments or simply protecting sensitive customer information. Compliance isn't just about avoiding fines, it's about protecting trust.

Even if you're not in a highly regulated industry, your customers still expect you to safeguard their data. Falling short can damage your reputation just as much as it can hurt your bottom line.

Make sure to:

- Review your policies regularly to ensure they match current regulations.
- Keep records of training and system updates.
- Make compliance a shared responsibility, not just an IT checkbox.

3. Continuity

If your systems go down tomorrow, how quickly can your business get back up and running? Continuity is all about being prepared.

Always:

- Make sure backups are running automatically and tested regularly.
- Have a plan in place for what to do if ransomware locks up your files.
- Practice your recovery steps before you need them.

4. Culture

At the end of the day, your people are your first line of defense. Building a culture of security means making good cyber habits part of everyday work.

Some ways to make that happen are:

- Encourage strong, unique passwords (or, even better, password managers).
- Require MFA (multifactor authentication) on all accounts that support it.
- Recognize employees who catch phishing attempts. This reinforces good habits and makes security a team win.

When security feels like a team effort, everyone gets better at it.

Security Is Everyone's Job

Keeping your business safe isn't just about software or hardware – it's about people. By building strong habits around communication, compliance, continuity and culture, you're not just avoiding threats, you're creating a workplace that takes security seriously every day.