THE HD TECH WAY

Insider Tips To Make Your Business Run Faster, Smoother, and More Profitably

CYBERSECURITY

PREVENTION VS. PREPAREDNESS

WHY REAL CYBER RESILIENCE REQUIRES BOTH

Your monthly newsletter, written for humans not geeks.

When most organizations think about cybersecurity, they think about prevention—firewalls, antivirus, email filtering, and keeping bad actors out. **Prevention is critical, but it is only half of the equation.**

True cyber resilience comes from understanding the difference between preventing an attack and being prepared when one inevitably happens. In today's threat landscape, the question is no longer if a cyber incident will occur—but when.

1. What is Cybersecurity Prevention?

Prevention focuses on stopping threats before they enter your environment. These are the tools and controls designed to reduce risk and block known attack methods.

Examples of prevention include:

- Firewalls & Secure Network Configurations
- Endpoint Protection & Malware Protection
- Email security & Phishing filters
- Multi-Factor Authentication
- Patch Management & System Updates

Prevention is essential. It reduces your attack surface, stops automated threats, and eliminates many common vulnerabilities.

2. Why Prevention Alone Falls Short

Cyber threats evolve faster than any single tool can keep up with. Zero-day exploits, social engineering, credential theft, and human error regularly bypass even well-designed preventive controls.

Even organizations with strong security stacks experience compromised user accounts, ransomware infections, data exfiltration, and business-disrupting outages.

Prevention reduces the likelihood of an incident—but it does not eliminate the impact when one occurs.

3. What is Cybersecurity Preparedness?

Preparedness assumes that a security incident will happen and focuses on minimizing damage, downtime, and business disruption when it does.

continued on page 2...

...continued from cover

3. What is Cybersecurity Preparedness? (cont.)

Preparedness is not a tool—it's a strategy built on people, process, and technology.

Preparedness includes:

- Incident response planning and documented playbooks
- Backup and disaster recovery strategies that are tested
- Security monitoring and rapid detection
- Employee training and role clarity during incidents
- Defined escalation paths and decision ownership

Prepared organizations don't just react—they execute.

4. Preparedness vs. Prevention: A Simple Analogy

Think of cybersecurity like fire safety in a building. Prevention is smoke detectors and fire-resistant materials. Preparedness is fire drills, evacuation plans, extinguishers, and insurance.

A building with only smoke detectors but no evacuation plan is not truly safe.

5. The Cost of Being Unprepared

Organizations that focus only on prevention often struggle during incidents because no one knows who is in charge, decisions are delayed, backups fail, and communication breaks down.

The result is longer downtime, higher recovery costs, reputational damage, and increased legal exposure.

6. Cyber Resilience Lives at the Intersection

Cyber resilience is not choosing prevention or preparedness—it's deliberately investing in both.

A resilient cybersecurity strategy prevents what it reasonably can, detects what it can't prevent, responds quickly, and recovers operations with minimal disruption.

The Bottom Line

Prevention is about keeping threats out. Preparedness is about staying operational when something gets in.

Organizations that understand this distinction move from a fragile security posture to a resilient one—ready to withstand, respond, and recover from cyber incidents without crippling the business.

Technology Update

Microsoft Teams Should Feel *Faster & More Reliable*

Microsoft has confirmed a behind-the-scenes performance upgrade for Teams on Windows. And it's more important than it sounds.

Teams is being re-engineered so that call handling (one of its most demanding tasks) runs in its own dedicated process.

By separating calls from the rest of the app, Teams should start faster, use system resources more efficiently, and deliver smoother meetings.

There's no change to how Teams looks or works, but you may need to update security or device management tools, so the new process isn't mistakenly blocked.

NEW TO

Microsoft

Copilot gets smarter (again)

Microsoft is rolling out a set of practical upgrades to Copilot designed to make it more useful for everyday work.

Soon you'll be able to pin important conversations so they don't get lost, work with much longer chunks of text, and ask Copilot to summarize lengthy chats or turn them into usable documents.

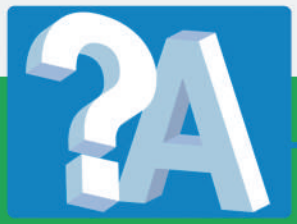
Copilot is also gaining a more advanced memory feature. It can remember helpful details from past conversations, with clear controls so you can see, manage or delete what it remembers.

These updates are inspired by how Microsoft CEO, Satya Nadella, uses Copilot. They're already gradually rolling out.

INSPIRATIONAL QUOTE OF THE MONTH

"Don't be intimidated by what you don't know. That can be your greatest strength and ensure that you do things differently from everyone else."

Sara Blakely, businesswoman and philanthropist.



Q: Should we use AI tools in our business, or wait until things settle down?

A: Start now. The key is using approved tools, setting clear rules, and making sure your data is protected.

Q: Do we need to control which apps staff can install?

A: Yes. Unapproved apps may store data insecurely or create hidden risks. A managed app list keeps everything safer and easier to support. Individual users should *not* have the ability to install software.

Q: What does zero trust mean?

A: It's a security approach where nothing is trusted by default. Users can authenticate, but the devices are *not* trusted by default. In Star Wars Episode VI (*Return of the Jedi*), old codes are given to access Endor. With Zero Trust, the shuttle full of rebels would've been swept & searched. "Flying Casual" couldn't get past Zero Trust.

Upcoming Event:

HD Tech Tower Talks: Practical, Implementable AI Tips

Thursday, May 7th, 2026
Long Beach Yacht Club, 4:30-6:30PM

Key Speakers:
Tom Hermstad (HD Tech)
Sean Patterson (StartGuides)
Dave Cunningham (Alvaka)

We're hosting an AI roundtable, where local business leaders and AI experts will share their real, actionable tips for better AI adoption and implementation. Tom will help you learn how to adopt AI safely, strategically, and in a measured manner. Sean will speak more on executive AI use in the workplace, where you can go and where you can be with successful AI adoption. Last, but certainly not least, Dave will speak on AI as it relates to the ever-changing landscapes of Ransomware and Cybersecurity.

For an invite, email info@hdtech.com and put HD Tower Talks in the Email subject line.

This is how you can get in touch with us:
CALL: (877) 540-1684 | EMAIL: info@hdtech.com
WEBSITE: www.hdtech.com

AI ADOPTION

THE REAL REASON YOU'RE STRUGGLING WITH AI

AI has become a regular topic in business conversations.

It comes up in meetings, strategy days and vendor pitches.

Yet for all the talk, many organizations are still struggling to turn AI from an interesting idea into something that genuinely helps people do their jobs.

In many organizations, AI is stuck in a trial phase.

Someone experiments with a tool. A small pilot runs for a few weeks. Then progress slows. The AI works, but businesses struggle to move from experimentation to everyday use. The return on investment everyone expects stays just out of reach.

Uncertainty is usually to blame.

Leaders worry about security, privacy and compliance. They're unsure what data AI tools are allowed to see or how decisions are being made. Others admit they don't yet have a clear business case, so AI becomes something interesting rather than something essential.

Another big factor is confidence.

Many employees are curious about AI, but also nervous. They worry about making mistakes, relying on the wrong answers, or using tools incorrectly.

Without clear guidance, people either avoid AI altogether or use it quietly and inconsistently. That creates risk and limits the benefits.

It's a shame, because when AI is used properly, the gains are very real. Teams can respond to customers faster, spot issues earlier, analyze data more easily and reduce time spent on repetitive admin.

In technical areas, AI can help monitor systems, improve security, and surface problems before they turn into outages. These are practical, everyday improvements that add up quickly.

The businesses seeing progress tend to take a steady, human-first approach. They set clear rules around how AI should be used, what it can and can't do, and where human judgement still matters. They focus on giving staff training and reassurance, not just new tools.

AI becomes a support act, not a replacement.

AI projects don't usually stall because the technology isn't ready. They stall because people aren't.

BUSINESS GADGET OF THE MONTH

Plaud Note AI Voice Recorder

If you spend a lot of time in meetings in-person or in calls without a headset, this could save you hours.

It's a small voice recorder that uses AI to turn conversations into clear summaries, transcripts and even meeting notes within minutes.

You press record, have your meeting, and Plaud does the rest. It runs on its own battery, so it won't drain your phone, and lets you jump back to exact moments in the audio if you need to double-check details.

$159 from Amazon.

Need help with that? **Get in touch.**