# THE HD TECH WAY

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


**How do you imagine a cyberattack?**

A sophisticated hacker breaking through layers of security? Using advanced tools that no regular business could possibly defend against?

The reality is usually way less glamorous.

Many breaches start with something small. A forgotten account that was never removed. A laptop that missed an update. A security setting that was switched off and never switched back on.

These are the kinds of gaps attackers actively search for because they're far easier to exploit than forcing their way through a heavily protected system.

In other words, the danger often comes from the things nobody realized were a problem.

One of the biggest changes in cybersecurity right now is the growing focus on identities.

Instead of attacking systems directly, criminals increasingly target usernames and passwords.

Once they gain access to a legitimate account, they can move through a business much more easily because, from the outside, it looks like a normal user logging in.

That can happen surprisingly quickly. In some cases, ransomware attacks have escalated within hours of the initial breach.

The challenge is that modern businesses are complicated.

Staff work remotely. Devices move between home and office. New software gets introduced. Small gaps appear naturally, unless someone is constantly monitoring them.

Even security tools themselves can become blind spots.

You may have protection installed, but if it is misconfigured, outdated, or partially disabled, it creates a false sense of security.

Attackers also rely heavily on something known as "living off the land" techniques. This means using legitimate tools already built into Windows and Microsoft 365 to carry out malicious activity.

*continued on page 2...*

*...continued from cover*

Because those tools are commonly used by IT teams every day, suspicious behavior can blend into normal activity more easily.

**Artificial Intelligence is likely to accelerate this problem.**

AI tools can help criminals identify weaknesses faster, automate attacks, and adapt techniques more quickly than before.

But many of the most effective protections are still the basics done well. Strong passwords, multi-factor authentication, regular OS updates, controlled access permissions, and ongoing staff awareness training remain some of the strongest defenses available. A proper cyber security perimeter with monitoring coupled with user awareness is still the best combination at preventing successful cyber attacks.

If you'd like help spotting and closing small security gaps before someone else finds them, **Get in touch.**

## INSPIRATIONAL QUOTE OF THE MONTH

*"If you're not failing every now and again, it's a sign you're not doing anything very innovative."*

**Woody Allen,**
**filmmaker and actor.**

## Debug your tech knowledge for this month's quiz...

1. What was the first item to be scanned using a barcode?
2. Which company popularized the term "Tablet PC" in 2001?
3. What was the name of the first social networking site launched in 1994?
4. What was eBay.com originally called?
5. What is a technical term for the "brain" of the computer?

The answers are below.

1.Wrigley's gum
2.Microsoft
3.GeoCities
4.Auctionweb
5.CPU (Central Processing Unit)

## ?A ANSWERS BY: TOM HERMSTAD, YOUR CYBER LIFEGUARD

**Q: Is it safe to use personal devices for work email and files?**

**A:** It depends on how they're set up. The risk isn't the device itself — it's that personal phones and laptops usually don't have the same security controls as company equipment. No Mobile Device Management (MDM), no encryption enforcement, no way to wipe it remotely if it's lost or stolen. If your team uses personal devices, we should talk about a basic policy to cover the gaps.

**Q: How long is too long to go without a security update?**

**A:** More than 30 days is risky. Most attacks exploit known vulnerabilities that already have a patch available — attackers count on people not applying them.

**Q: How do we know our backups are actually working?**

**A:** You don't — unless you test them. A backup that's never been restored is just an assumption. We recommend doing a test restore at least quarterly. It doesn't have to be the whole system — even restoring a single folder confirms the process works. If you're not sure when yours were last tested, ask us and we'll let you know. Each day we monitor backups; we also test that the backup is actually usable. Monitoring + verification = good backups.

# STRATEGIC EXECUTION SERIES

## PART 4: EXECUTION AT THE INDIVIDUAL LEVEL

GREAT STRATEGIES ARE EXECUTED ONE PERSON AT A TIME

Thomas H. Willingham,
The Hampton Group
tomw@thampton.com

In Part 3, we explored how successful organizations execute by creating clear goals, defining actions, measuring progress, and fostering accountability. Those systems are essential—but execution ultimately happens at the individual level. Organizations don't execute. People do.

No matter how well-designed a strategy may be, success depends on each employee understanding their role and consistently following through. Leaders play a critical role in creating an environment where individuals are prepared, empowered, and committed to succeed.

### Three Ways Leaders Improve Individual Execution

**1. Create Clarity Around Goals & Actions:** People perform best when they understand exactly what success looks like. Clearly defined goals, measurable expectations, and specific action steps eliminate confusion and help employees connect their daily work to organizational priorities. **Clarity creates alignment, and alignment drives execution.**

**2. Ensure Employees are Ready, Willing, & Able:** Early in my career, I competed in triathlons. Success required more than motivation—it required the training, conditioning, equipment, and discipline to perform. Today, while I may still be mentally ready and willing, my body reminds me that ability also matters. The same principle applies in business. Employees must be **ready** through clear direction, **willing** through engagement and purpose, and **able** through training, resources, and the authority to make decisions. When people lack any one of these elements, execution suffers.

**4. Build Commitment, Not Just Promises:** We make promises every day: "*I'll finish the report next week*" or "*I'll be there at 10:00.*" A promise reflects good intentions, but good intentions alone don't consistently produce results. Kierson and Tomlinson, in *Discovering Execution*, make an important distinction: "Think of a **commitment as a declaration** that you're going to do something or accomplish something."

Unlike a simple promise, a commitment requires thoughtful planning, clear priorities, coordination with others, and consistent follow-through. It creates accountability not only to the outcome, but also to the actions required to achieve it. **Organizations that cultivate genuine commitment consistently outperform those that rely on good intentions alone.**

### The Takeaway

Strategic execution begins long before results appear on a dashboard. It starts when leaders provide clarity, equip employees to succeed, and build genuine commitment to shared goals. When individuals consistently execute well, teams perform better. When teams perform better, strategies become results.

**Great organizations aren't built on promises; they're built on people who make commitments and deliver on them.**

## DID YOU KNOW...

that might not really be support?


The FBI has warned businesses about a cybercrime group pretending to be IT support staff.

Attackers have reportedly gone as far as turning up in person at offices after first contacting staff by phone. They pose as technicians fixing a problem, then copy sensitive files onto external drives and install malware in the background.

Staff awareness and clear verification processes for visitors and support requests are just as important as technical security controls.

**WANT THE FULL ARTICLE? CHECK OUT OUR BLOG!**


**AI tools are becoming a normal part of the working day.**

Someone uses one to tidy up a report. Someone else asks a chatbot to summarize meeting notes. A team member installs an AI browser extension because it helps them work faster.

Most of this happens with good intentions.

But some businesses have no visibility of it at all.

This is known as "shadow AI".

It describes employees using AI tools that haven't been approved, reviewed, or properly managed by the business.

In many ways, it's like shadow IT, where staff adopt their own software without involving the IT team.

The difference is that AI tools can interact with company information in deeper ways.

Employees may paste confidential documents into public chatbots, connect AI assistants to email accounts, or allow AI tools to access files and calendars without fully understanding what happens to that data afterwards.

The motivation is easy to understand. These tools save time, reduce admin, & help people get through work more efficiently.

So, banning AI outright rarely works.

If employees feel the tools genuinely help them, they often continue using them secretly. At that point, the business loses even more visibility and control.

The better approach is usually to accept that AI is now part of modern work, then guide people towards safer, approved options.

Newer AI systems are becoming more capable very quickly. Tools are no longer limited to generating text or summaries. They can search files, access systems, organize information, trigger workflows… and even carry out actions automatically.

Without proper oversight, that creates obvious security and compliance concerns.

For businesses using Microsoft 365, approved tools like Copilot offer a safer route because they sit inside existing permissions and security controls. Other tools can be employed to only allow users to use specific AI tools. Please let us know if you want to discuss this.

That doesn't remove risk completely, but it does give businesses much better visibility over how AI is being used.

Whatever tools you're using, the important thing is not to ignore the issue.

## PRODUCTIVITY TOOL OF THE MONTH

### Power Automate

You know those small repetitive jobs that eat away at your day?

Renaming files, sorting attachments, copying information from one place to another, opening the same apps every morning….

Power Automate, built into Windows 11 Pro, can handle those kinds of tasks automatically.

And better yet, you don't need to know how to code. You can create simple automations using drag-and-drop tools or even record yourself doing a task once and let Power Automate turn it into a reusable workflow.

It's one of those tools many businesses already have but rarely realize how much time it could save them.

If you are interested in hearing more about PowerAutomate, Ask Us!

**If you need better oversight on how your team is using AI tools, we're here to help!**

Get in touch.