July 2026

Tech Times

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

How to Calculate What an Hour of Downtime Really Costs Your Business

If your systems went down for an hour tomorrow, what would it cost you?

When asked this question, most business owners pause and guess a number that is almost always too low. The costs of downtime don't appear neatly in a report. They scatter across your day in ways that are easy to miss unless you sit down and map them out.

The back-of-the-napkin downtime calculation

These four simple components provide a real number you can plan for.

1. LOST REVENUE

Divide your annual revenue by 2,000, the approximate number of working hours in a year. If you bring in $2 million a year, that's around $1,000 per business hour.

Your number: $___ per hour

2. IDLE EMPLOYEES

Count the employees who can't do their jobs when systems go down. Multiply their average hourly cost by the number of people affected. Ten employees at $30 per hour means $300 sitting idle.

Your number: $___ per hour

Now add the **$**___ per hour in lost revenue and the **$**___ per hour for idle employees.

This **$**___ per hour is your subtotal.

3. RECOVERY TIME

Here's the one most people miss. When systems come back online, things don't snap back to normal. A one-hour outage rarely costs just one hour. A conservative rule of thumb is to add 50% for recovery.

Multiply your subtotal by 1.5 to get your estimated downtime event cost **$**___

4. CUSTOMER IMPACT

Think about what happens on the customer side when you go dark.

Missed calls. Failed transactions. A customer who reached out at a critical moment and hit a dead end. Some of those people quietly move on without ever telling you.

Ask yourself: What's one lost customer worth to you?

A QUICK EXAMPLE AND WHAT IT REVEALS

Take a 20-person accounting firm bringing in $3 million a year. Lost revenue is about $1,500 an hour.

Add 15 idle employees at roughly $450 per hour each to the total, and so far, they're at $8,250.

Apply the recovery multiplier and one hour of downtime costs over $12,000 before a single customer relationship is factored in.

Key Takeaway:
For most businesses, a full year of prevention costs less than recovery from a downtime event.

The Most Dangerous Risks Don't Swim on the Surface

On the surface, the water looks calm. That's what makes Shark Week fascinating every year. The danger is never visible on the surface. It's what's already moving underneath.

Cybercriminals operate the same way. The threats businesses face are designed to blend in with usual operations until the moment something breaks, money moves or systems go down.

During the summer months, when schedules shift, employees travel and oversight gets thinner, cybercriminals know businesses are often paying less attention.

Here are three ways they're circling right now.

1. FAKE INVOICES AND VENDOR IMPERSONATION

Attackers don't need to hack anything. In many cases, they need to send just one believable email. The email arrives looking completely normal, someone on your team pays the "vendor," and by the time anyone realizes the request wasn't legitimate, the damage is done.

These attacks spike during vacation season for a simple reason. When the person who normally approves payments is out, requests get rerouted to people who don't always know what normal looks like. Temporary stand-ins are less likely to question urgency and attackers know it.

The fix is simple to implement: Build a verification process for any financial request received via email. A quick confirmation call to a known number, not the number listed in the email, is enough to stop most of these before they go anywhere.

2. PHISHING ATTACKS THAT TARGET DISTRACTED EMPLOYEES

Phishing works because it's engineered around how people behave when they're busy. Cybercriminals design these moments moments deliberately. A distracted employee sees a password reset notification and clicks the link. Someone gets a text that looks like it came from IT. An email lands right before a meeting asking for urgent approval on a wire transfer. Nobody stops to verify because stopping feels like losing time.

The most effective protection isn't a software solution; it's culture. Employees need to feel comfortable slowing down when something seems off. Speed is a weapon attackers use against you. Slowing down is how you take it away from them.

3. THIRD-PARTY RISKS THAT TRAVEL FAST

When a vendor with access to your systems is compromised, the threat doesn't stay contained to them. It travels directly into your environment through whatever connection they have to your business.

This is supply chain exposure, and most businesses have significantly more of it than they realize.

Outsourcing a service doesn't outsource accountability.

Knowing where you stand with supply chain exposure means being able to answer three questions:

1. Which vendors can access your data or systems?
2. What are they connecting to?
3. Who is responsible internally for managing those relationships?

Key Takeaway:
Sharks don't announce themselves and neither do the cybercriminals targeting your business right now.

The companies that get hit aren't always the ones that ignore obvious warning signs. They are the ones that assume everything is fine because nothing looks wrong.

5 Questions Most Business Owners Can't Answer About Their Systems

You don't need to be an IT expert to run your business, but you must be able to answer a few basic questions about the systems you rely on. If you can't answer them with confidence, you have gaps you need to close.

1. WHO HAS ACCESS TO YOUR CRITICAL SYSTEMS, AND IS IT STILL APPROPRIATE?

Think about your accounting software, your CRM and your email platform. Do you know who currently has login access to them?

Access grows over time. A contractor gets added. A former employee doesn't get removed. Someone's permissions expand for a one-time project and never get scaled back. Before long, more people have access than you realize, and some of them probably shouldn't.

This isn't about distrust.

Every unnecessary login is a security risk. A compromised credential gives someone a way in. The greater amount of unreviewed access, the harder it becomes to contain issues when something goes wrong.

2. IF SOMETHING BREAKS, WHO IS RESPONSIBLE FOR FIXING IT?

Pick any critical system in your business. If it went down today, do you know exactly who owns the response?

If the answer is "it depends" or "I'm not totally sure," you've identified a gap. When multiple vendors or team members are involved, accountability has a way of falling through the cracks. Everyone assumes someone else is handling it, and nothing gets handled.

Downtime costs money. Confusion about who to call makes that downtime longer. The time to figure out who owns what is before something breaks.

3. WHEN WAS THE LAST TIME YOUR BACKUPS WERE TESTED?

Setting up a backup is one thing. Making sure it can restore your data when you need it is something else entirely.

Backups are usually configured once, checked off the list and quietly forgotten. A backup that has never been tested is not a safety net.

If you can't remember the last time a backup was tested, you're relying on blind trust.

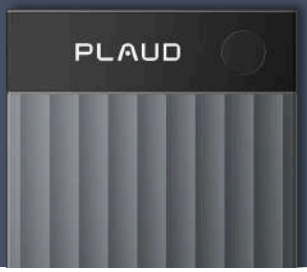
GADGET OF THE MONTH

Plaud Note Pro

Capture Every Conversation, Skip the Notes

If your day runs on conversations, this changes how you keep up.

The Plaud Note Pro is credit-card thin, but what sets it apart is the "press to highlight" button. Tap it during a meeting, and the AI prioritizes that exact moment later. It records from up to 16 feet away, auto-detects calls vs. in-person conversations, and turns everything into structured summaries, tasks and insights.



Your Midyear IT Review

Small gaps build quietly as businesses grow. Check where you stand:

- ☐ Do you know who has access to your systems?
- ☐ Have your backups been tested recently?
- ☐ Do you know what your vendors can access?
- ☐ Is it clear who is responsible when something goes wrong?
- ☐ Do your systems still support how your business runs?

If you answered no to any of these, your business needs more attention.

4. WHERE DOES YOUR BUSINESS DATA LIVE TODAY?

Data doesn't stay in one place. It spreads.

New tools get added over time. Files end up in email threads, shared drives, project management apps and personal folders. Some live in tools you signed up for years ago and rarely touch anymore.

When you don't have a clear picture of where your data is, you lose clarity on who can see it, how it's protected and what happens if something goes wrong.

5. WHICH VENDORS HAVE ACCESS TO YOUR SYSTEMS OR DATA?

Vendors get added quickly. An integration here, a new app there, a tool someone on your team recommended. Each one often comes with some level of access to your systems or data.

Vendors having access to your data isn't the problem. Not knowing what they can see or do with it is. Third-party access introduces risk from outside your business, and it tends to get the least scrutiny of anything on this list.

A useful question: if you listed every vendor with access to your systems right now, would you know what each one can see or touch?

IF YOU CAN'T ANSWER THESE QUESTIONS, IT'S TIME TO ACT

These aren't obscure technical questions. They're the basics: access, accountability, backups, data and vendors.

Finding answers now means fixing them before they cost you. Review your systems, clarify responsibilities and check your backups. These small steps now can prevent major headaches later.

Key Takeaway:

These five questions don't require technical expertise to answer. If you're unsure about any of them, take the initiative to investigate and strengthen your business's systems. Your future self will thank you.

Cartoon of the month

"When fireworks show signs of quiet quitting."

COMING NEXT MONTH

TEST YOUR SAFETY NET BEFORE YOU NEED IT

Every business depends on systems that could fail. The real question is whether yours would recover quickly when that moment arrives.

Next month, we're looking at how the most resilient businesses test and monitor their systems long before anything goes wrong. When your safety net is checked regularly, a disruption stays manageable instead of turning into something much harder to come back from.