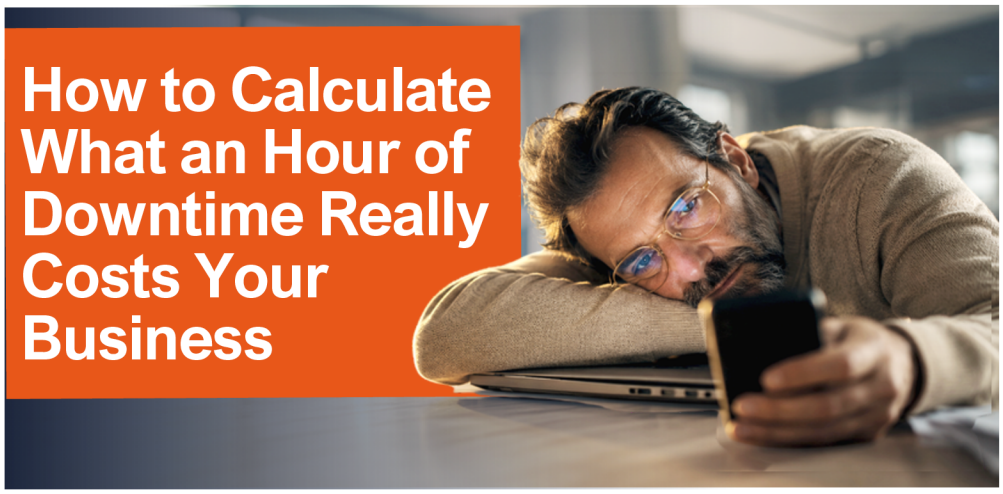
July 2026

GIO Tech Times

Putting the Power of IT Back in Your Business with Insider Tips for Speed, Simplicity, and Profit



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

Most business owners know downtime is expensive, but few know what it actually costs. Use this simple exercise to estimate the real financial impact of an outage.

A quick way to estimate what downtime could cost your business:

1. LOST REVENUE

Divide your annual revenue by 2,000 (the average number of working hours in a year). $___ per hour

2. IDLE EMPLOYEES

Calculate the hourly cost of employees who can't work during an outage.
$___ per hour
Subtotal: $___ per hour

3. RECOVERY TIME

Getting systems back online doesn't mean you're instantly back to normal. A good rule of thumb is to add 50% for recovery and catch-up time.

Estimated downtime cost:
Subtotal × 1.5 = $___

4. CUSTOMER IMPACT

Don't forget the harder-to-measure costs: missed calls, delayed service, failed transactions, and potential lost customers.

EXAMPLE:

A 20-person accounting firm generating $3 million annually loses about $1,500 per hour in revenue. Add employee downtime and recovery time, and a single one-hour outage can easily exceed $12,000 before customer impact is even considered.

POWERING IT *with Dan*

The Mid-Year IT Check

We're halfway through the year - a natural moment to ask: is your technology actually working for your business, or just working? There's a difference. And most businesses don't find out which one they have until something breaks.

Downtime doesn't wait for a convenient time. It shows up on your busiest day, costing you productivity, customer confidence, and trust that takes years to build.

What I see time and again: businesses uncovering gaps only after something forces their hand - and by then, recovery is already underway. It's always more costly than prevention. A mid-year IT review changes that equation. Test your recovery plan. Review your cybersecurity and check vendor agreements. Small adjustments you make today are the crises you don't deal with tomorrow.

For our clients, this is built into how we work together year-round. If you're not yet a GIO client and want that peace of mind heading into Q3, let's talk.

Dan Giordano
dan@giotechnologies.com

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 re-routed 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.

TEAM GIO

Powered by Bryan

What Your Business Doesn't See - But Should

After years in the field, I can tell you most businesses have no idea what's actually running on their network. Unpatched systems, end-of-life software still handling live data, personal devices connecting to company resources with zero oversight. These aren't hypotheticals. I see them every week. And in most cases, the business had no idea until we ran a full assessment.

The bigger issue? Unclear ownership. Nobody knows who manages the firewall. Nobody knows when the last backup actually completed or if it's even restorable. That uncertainty is a serious liability.

This is where GIO Technologies changes everything. We're not just fixing things when they break. We're monitoring endpoints, patching vulnerabilities, and making sure someone is accountable for every layer of your IT environment.

You shouldn't need to understand subnets and security policies to run your business. That's our expertise at GIO Tech. We've built our reputation on catching the problems you didn't know you had before they catch you. Our motto is "Put the Power of IT Back in Your Business" - and you can't do that if you're constantly worried about how your IT is performing.

-Bryan Clarke
support@giotechnologies.com

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.

Newest Member of Team GIO

We're excited to welcome Tersh Baseman to the GIO team as our newest IT Support Engineer! Tersh brings years of field experience, a sharp eye for detail, and a genuine commitment to customer service. We're thrilled to have him on board - our clients are in great hands. Welcome to the team, Tersh!

GIO MONTHLY MOMENTS

TEAM GIO🥎🧡

Team GIO traded keyboards for softball gloves and joined Tar Heel Construction Group for their annual charity softball tournament benefiting the local recreation council. While we may not be adding any championship banners to the office, we had a great time supporting a great cause, spending time with friends and community partners, and showing off a few flashes of athleticism along the way.

NEW OFFICE UPDATE

The new GIO office sign is officially up, and the landscaping is in place, making the property look more like home every day. There's still plenty of work ahead, but it's exciting to see everything starting to come together. Now we're hoping the inside renovations will begin soon so we can continue transforming the space into a place that reflects our team, our clients, and the future of GIO Technologies.

GIO GIVING BACK

At GIO, we believe supporting our clients goes beyond technology support. We were honored to donate conference room technology, including a computer, TV, webcam, speakers, and accessories, to help Harford Family House create a more connected and collaborative meeting space. We're proud to support the incredible work they do in our community and grateful for the opportunity to be a small part of their mission.