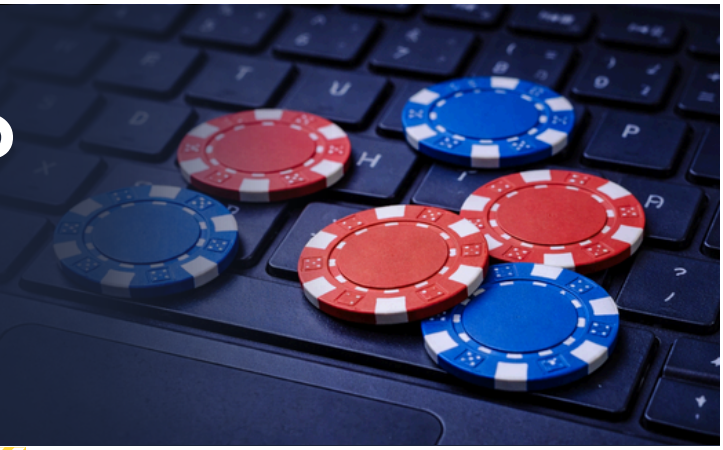
TECHNOLOGY TIMES

APRIL 2026

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

# FEELING LUCKY?

## THAT'S NOT HOW WELL-RUN BUSINESSES OPERATE



While luck may play a role in celebrations or games, respected organizations understand that success is built on strategic planning and sound management, not chance.

No experienced owner would ever say:

- "Our hiring strategy is whoever walks in."
- "Our sales plan is hoping customers find us."
- "Our accounting approach is the numbers working themselves out."

That would be absurd.

### The Quiet Double Standard

Yet, when it comes to technology, even sophisticated organizations can fall into a pattern of complacency.

*"We've never had an issue before."*
*"It's probably backed up somewhere."*
*"We'll deal with it if something happens."*

These are not strategies. They are hopeful assumptions, risk disguised as readiness. Unless your IT systems are managed by a magician, relying on luck is not a sustainable plan, it's a risky bet.

Most owners would never leave payroll, taxes or customer service to chance. Yet, when it comes to technology resilience, hope often stands in for preparation.

### Why 'We've Been Fine So Far' Doesn't Hold Up

Here's the trap: When nothing bad has happened, it feels like proof that nothing will.

It's easy to mistake a lack of incidents for proof that your systems are secure. But every business that's faced a major disruption once felt "we've been fine" the day before.

Luck isn't a business continuity strategy. It's simply unmanaged risk waiting to surface.

Think of it like driving without insurance. You might get away with it for years, but the day something goes wrong, you'll wish you had a plan.

### Prepared vs. Hoping for the Best

Most businesses often only discover their vulnerabilities in the midst of a crisis. That's when critical questions arise:

- Do we have a backup?
- How recent is it?
- Who handles this?
- How long will we be down?

Proactive businesses have clear answers to these questions. Those relying on luck find out the hard way, in real time.

Being prepared doesn't mean expecting constant disasters. It means having tested, transparent, documented systems so that even minor issues are handled efficiently and without disruption to clients or staff.

Without preparation, small technical hiccups can escalate into major operational crises, affecting client trust, employee morale, and ultimately, your firm's reputation.

Suddenly you're spending more time fixing problems than running your business.

### The Reality Check

If your accountant managed books the way you manage tech recovery, would that be acceptable? Why treat technology differently?

Consistent standards across all business areas ensure reliability and peace of mind, protecting your firm's assets and reputation. It's time to bring the same rigor to technology that you apply everywhere else.

**To view our full library of newsletters go to:**
www.sysoft.ca/newsletters
or scan the QR code

# YOUR ACCOUNTANT IS STRESSED.

## HACKERS KNOW IT.


Your accountant is buried. Your bookkeeper is scrambling. Deadlines are looming. Emails are flying faster than anyone can keep up. Everyone is heads down, trying to get through tax season. This isn't news to you, and it's not news to hackers either.

Phishing attempts surge during tax season. Their messages aren't dramatic. They blend in with everyday business requests, right when people are busiest. That's not coincidence. That's strategic timing.

### The Stressed Supply Chain

Here's what most people miss: Hackers aren't just targeting accounting firms; they're targeting the chaos around them.

**During tax season:**

- Clients rush to send sensitive documents
- Staff shortcut normal checks to keep up with volume
- "Just send me the file" replaces usual caution
- Verification gets skipped because everyone is slammed

The whole ecosystem speeds up, making mistakes more common. Hackers don't go after calm, methodical businesses. They go after the busy ones.

### What These Attacks Look Like

This isn't a movie plot. It's an email that looks exactly like the others in your inbox:

- A message from "your accountant" asking you to resend documents because something didn't come through
- A note from a vendor saying their bank information has changed and needs updating
- A DocuSign request that "needs your signature today"
- An urgent email from "your CEO" who's traveling and needs help immediately

None of these feel suspicious. They feel like normal business. That's why they work.

### Why Busy People Get Caught

Falling for these scams isn't about being careless. It's about being human. When inboxes are full and deadlines are tight, people don't read carefully. They scan. They assume. They react.

Bad actors know this. Their messages are designed for people who are moving too fast to notice the one detail that's off. They don't need you to be reckless. They need you to be busy.

### 4 Simple Ways to Avoid Being an Easy Target

You don't need fancy tools or a security team to reduce your risk. You just need a few intentional habits during busy months.

**1. Verify payment changes by phone**

If an email says a vendor's banking details have changed, don't reply to the message. Call a number you trust to verbally confirm.

**2. Slow down requests for sensitive information**

Urgency should be a signal to pause, not to rush. If someone asks for bank statements, tax documents or other financial files "right now," take a moment to verify.

**3. Confirm urgent requests through a second channel**

If an email claims something is urgent, verify it another way. A quick call, text or internal message can stop a bad decision before it starts. Real urgency can survive a two-minute check.

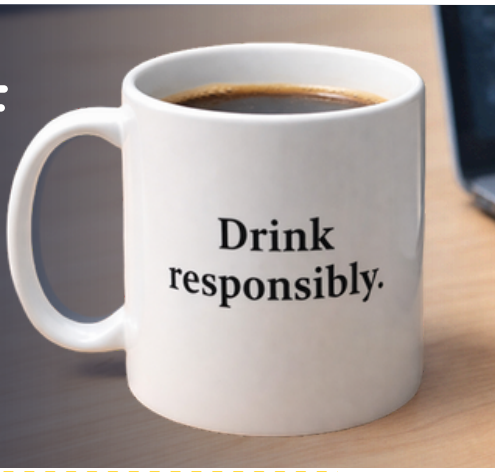
**4. Give your team a five-minute heads-up**

Remind your team that it's okay to slow down, double-check and ask questions when something feels off. That small permission shift can prevent a lot of unnecessary cleanup later.

### The Takeaway

The attacks showing up during tax season aren't clever. The power is in their timing. You don't have to overhaul your systems to avoid becoming the easy target, but you do need to slow down when it matters and verify when things feel urgent.

# HOW A CUP OF COFFEE CAN TAKE DOWN YOUR WHOLE BUSINESS




Picture the start of a typical workday: coffee in hand, laptop open, ready to tackle critical client matters and project deadlines. The office hums with focus, and everyone's routine feels comfortably predictable.

Suddenly, your elbow nudges the mug.

Time slows just enough for you to watch coffee spill across the keyboard and disappear into places coffee should never go.

The screen flickers.
The keyboard becomes unresponsive.
Your device makes an alarming noise.

There's no cyberattack, no ransomware, no urgent warning—just a normal moment turned upside down by an everyday mishap.

This completely normal moment that suddenly changes the day is how many business disruptions start. The smallest accidents creating a domino effect, impacting not just one person but entire teams and client deliverables.

## The Problem Isn't the Mistake — It's What Happens Next

Many firms imagine downtime as catastrophic: servers offline, critical systems inaccessible, productivity at a standstill.

In reality, downtime is often as mundane as a spilled drink, a file that "definitely got saved" but now doesn't exist, an update that doesn't finish or a computer that won't boot for any obvious reason.

The real productivity loss doesn't come from the mistake itself. It comes from the stall that follows: the uncertainty, the delay, and the question "do we know how long this will take?"

Work doesn't fully stop—it lingers in a half-productive state. For professionals, this can be as damaging as total downtime. Even brief interruptions can create stress, erode confidence, and put relationships with clients at risk.

## The Hidden Cost of Waiting

This is what a typical disruption looks like:

One employee can't work, so they wait. Colleagues attempt to help but aren't sure how. Someone notifies IT. Others shift to alternate tasks, hoping for a quick fix. Leadership may not even be aware of the issue until productivity has already dropped.

Ten minutes turn into thirty. Thirty turns into an hour.

Now multiply that by the number of people affected, the interruptions, the shifting mental focus mental and the momentum that never quite comes back.

Small delays compound quickly—not with dramatic headlines, but with quiet frustrations that sap productivity and client satisfaction .

...continued on page 4

## SHINY NEW GADGET OF THE MONTH

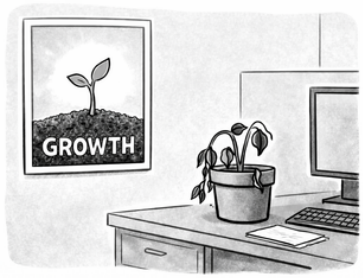
### Fieldy

Fieldy is a privacy-first, AI-powered wearable that securely captures in-person conversations allowing professionals to stay focused without needing to jot down notes or disrupt the flow of discussion so users can remain fully engaged.

Worn discreetly as either a pendant or wrist device, Fieldy operates hands-free. Leveraging AI, it transcribes conversations, highlights important decisions, and creates reminders—all seamlessly.

To safeguard sensitive discussions, Fieldy processes conversations without storing raw audio, ensuring leaders can trust that confidential information remains protected.

## CARTOON OF THE MONTH




"The poster is more aspirational..."

## FREE ASSESSMENT

### FREE Cybersecurity Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will conduct a comprehensive cybersecurity audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast.

This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

**To Get Started And Claim Your FREE Assessment Now, Call Our Office At 416-410-7268 or visit www.sysoft.ca/audit**

*...continued from page 3*

### Same Problem, Different Outcomes

Let's revisit the coffee spill scenario.

In one business, there's no clear protocol. Someone suggests calling "the IT expert," but they're unavailable. People wait for instructions. By midday, half the workday is lost. The lack of preparation and clarity means everyone is left guessing, wasting valuable time and energy.

In another firm, the issue is immediately reported, the response is clear and streamlined, files are restored, and the employee is quickly back to delivering client value. There's a sense of confidence and calm because everyone knows what to do.

Same incident. Same challenge. Entirely different outcomes.

The difference is not luck—it's clarity and speed in recovery. The right plan transforms potential chaos into routine business continuity.

### Why Leading Businesses Make Disruptions Routine

Here's what many firms overlook: You can't prevent every problem. That's unrealistic.

The real objective is to make disruptions routine and manageable. By having clear processes and designated roles, your team can respond calmly and quickly, minimizing the impact on clients and workflow.

Routine means no scrambling, no guesswork, no lengthy pauses, and no confusion about who is responsible.

When disruptions are handled efficiently, your firm stays focused and productive—clients notice professionalism, not chaos. This approach builds trust and strengthens your reputation as a reliable partner.

### This Is a Leadership Issue, Not a Technology Issue

When minor incidents cause major delays, it's rarely due to the tools themselves.

It's because:

- There's no consistent, reliable plan for actions following an incident
- Roles and responsibilities are ambiguous
- Recovery depends on the right person being available in a timely manner
- "Back to normal" isn't clearly defined, impacting consistent recovery and reliable outcomes

The frustration comes not from the error itself, but from the uncertainty that follows. Employees are left in the dark, unsure of what their next steps should be or who to turn to for help.

Well-run businesses eliminate that uncertainty.

They invest in clear recovery plans, communicate expectations, and empower their teams to act confidently when disruptions occur.

### A Simple Question Worth Asking

You don't need a dramatic audit to start thinking differently about this. Simply ask: If something small went wrong today, how quickly would your team be back to serving clients and advancing projects in a consistent, reliable way?

If the answer isn't clear, it's not a failure—it's an opportunity.

Use this insight to craft a strategy that minimizes downtime, streamlines recovery, and ensures your business continues to deliver exceptional client service, no matter what the day brings.

Even small, proactive improvements in preparation can make a big difference in maintaining productivity, morale, and a reputation for transparency and accountability.