

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



THE MOST DANGEROUS RISKS IN YOUR BUSINESS

Don't Swim On The Surface

On the surface, everything can look calm.

The biggest threats are not always obvious at first. They are often already moving quietly beneath the surface, showing up as small warning signs that are easy to overlook until they become a much bigger problem.

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

Summer can make that risk even greater.

With employees away, decision-makers harder to reach and day-to-day routines disrupted, attackers look for moments when teams are moving quickly and verification steps are easier to miss.

Here are three ways they're circling right now.

1. Fake Invoices and Vendor Impersonation

Attackers don't need to hack anything. They need just one believable email.

Business Email Compromise (BEC) works by impersonating a vendor, supplier or executive your team already trusts. The message may look routine: an updated banking detail, a revised invoice or a payment request that appears to come from someone familiar. By the time

anyone realizes it was not legitimate, the damage is done.

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

The Fix: Create a clear verification process for any payment change, new vendor request or financial instruction sent by email. Make sure employees know who to contact, what to confirm and that they will be supported for taking the extra step. A quick confirmation using a known phone number can prevent a costly mistake.

2. Phishing Attacks That Target Distracted Employees

Phishing works because it's engineered around how people behave when they're busy. A distracted employee sees a password reset and clicks. Someone gets a text from "IT." An email arrives before a meeting requesting urgent approval.

In busy professional environments, people often skip the second look because stopping feels like losing time.

The Fix: Employees need to feel comfortable slowing down when something seems off — an unexpected login, a payment instruction out of nowhere or a link they weren't expecting.

Encourage people to ask questions early instead of guessing under pressure. Speed is a weapon attackers use against you. A short pause, backed by a team that takes concerns seriously, is often what stops the attack.

3. Third-Party Risks That Travel Fast

Most businesses rely on outside providers, software platforms and contractors to keep work moving. But when a vendor with access to your systems or data is compromised, that risk can travel directly into your business. This supply chain exposure is often far greater than businesses realize.

Client files, financial information, email accounts and cloud applications can all be affected if access is not managed carefully. Trusted relationships still need clear ownership, regular review and practical controls.

Outsourcing a service doesn't outsource accountability.

The Fix: Answer these three questions:

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

If those answers aren't clear, your exposure is increasing your risk. ■

CELEBRITY SPOTLIGHT

HOW SMB LEADERS CAN BUILD A WORKPLACE PEOPLE DON'T WANT TO LEAVE

Arnie Malham on Growing Companies



Hiring is tough for small and midsize businesses. Good candidates have options, employees are more selective and SMBs often compete with larger companies offering bigger salaries, better benefits and clearer career paths.

So, how can your business stand out if you don't have the deepest pockets? Build a workplace people want to be part of.

That's what Arnie Malham, founder of cj Advertising and Legal Intake Professionals, learned while growing companies in a highly specific niche: advertising and intake services for personal injury law firms. Speaking to attendees of TMT's Q1 Producers Club meeting, Malham shared how difficult it was to recruit talent into an industry that wasn't always an obvious first choice.

"I had a business where recruiting was really hard," Malham said. "Creating a culture that gave people a reason to be at work was part of how we grew our business."

For leaders, that lesson matters. You may not be able to outspend larger competitors, but you can create a culture where people feel seen, valued and motivated to stay. And when good people stay, the whole business feels it. Customers get better service, teams work with less friction, and leaders spend less time replacing employees and more time growing the company.

Your Culture Is A Mirror

For years, Malham thought his culture problems were caused by everyone else.

"I spent years believing that the problem was my people. If only they understood. If they just came with a better attitude. If they just showed up when they were supposed to. It was all their fault."

But culture doesn't fix itself. It reflects what leadership allows, rewards, ignores and models every day.

"The bad news for everybody in this room is you are leadership," Malham said. "The culture you have right now, the one that exists in your company right now is the one you absolutely deserve and there is no way around it."

That may sting, but it's also empowering. If culture reflects leadership, leaders can change it.

Turn Culture From A Buzzword Into A System

According to Malham, one of the first steps in building a strong culture is giving it a name. A name makes culture more than a vague idea. It gives your team something to talk about, contribute to and protect.

At Malham's company, they called it "Camel Culture."

Camel Culture wasn't one single perk. It was a collection of rituals, rewards and habits that made the company feel distinct, including profit sharing, a dog-friendly office, a Better Book Club and tenure-based rewards.

That's an important point to understand: Culture isn't built through one big gesture. It's built through repeated moments that tell employees, "You matter here."

Employee Morale Is Customer Experience In Disguise

Malham also used morale surveys to understand how employees were really feeling. When he addressed the issues employees raised, morale improved. When morale improved, customer ratings improved, too.

A frustrated, burned-out team will eventually affect service quality, response times, sales conversations and customer retention.

Culture Is Not A Soft Issue

The takeaway is clear: You don't need flashy perks or a massive HR budget. You need a culture that is clear, consistent and true to the kind of business you want to run.

When your people want to stay, your customers feel it. When your customers feel it, your business is stronger. ■

6 QUESTIONS

Smart Companies Ask Their IT Provider Every Quarter

If the only time you speak with your IT provider is when a contract is up for renewal, you're doing it wrong.

Technology isn't a "set it and forget it" part of your business. It's constantly evolving and so are the threats that come with it. It supports client service, productivity, security, compliance and the day-to-day trust your clients place in your business.

That's why quarterly IT check-ins are non-negotiable. They create a regular opportunity to communicate clearly, confirm accountability and plan proactively before small issues become expensive disruptions.

The right IT partner should be ready to answer these questions in plain language, with practical next steps and a thoughtful understanding of your business goals.

Question 1: What security risks need our attention right now?

Every business has vulnerabilities, but not every risk carries the same level of urgency. The important question is whether your IT provider is actively identifying and addressing them before they become costly.

Ask them:

- Are there systems that need security patches?
- Have there been any unusual login attempts or suspicious activity?
- Are there users, devices or processes creating unnecessary risk?

You want specifics, not a generic "you're

protected" response. A strong IT partner communicates clearly, takes accountability for what they manage and helps your team understand where your biggest risks are today.

Question 2: Have you tested our backups recently?

A backup is valuable only if it works when you need it. That sounds obvious, but many businesses assume they're protected simply because backups exist. Then a server fails, ransomware hits or someone accidentally deletes critical data, and suddenly nobody's sure how quickly systems can be restored.

Ask:

- When was the last full recovery test?
- How long would restoration realistically take?
- Are backups stored securely and separately from our primary systems?
- Are cloud applications included in backup coverage?

You do not want guesses during an outage. You want a tested process, clear ownership and a team that can respond quickly when the pressure is on.

Question 3: Where is our technology slowing us down?

Most productivity issues don't look dramatic enough to trigger an IT emergency. They show up when your team loses momentum throughout the day.

An employee waits 15 seconds for an

...continued on page 4

SHINY NEW GADGET OF THE MONTH

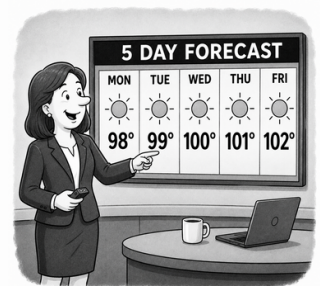
Your Laptop's New Best Friend:

UNITEK Adjustable Stand

Long days at your desk take a toll. This aluminum beauty features 360° rotation, adjustable height and a magnetic cooling fan to keep your machine chill during marathon work sessions. Ergonomic design reduces neck strain — perfect for video calls and back-to-back meetings. It's the kind of thing you don't think about until you have it, then you wonder how you ever worked without it.



CARTOON OF THE MONTH



"We're seeing a lot of consistency"

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



FREE DARK WEB SCAN

The Dark Web is Overflowing With Credentials... Are YOURS There Too?

Every day, these thieves are finding new ways to outsmart security, steal your passwords and wreak havoc on your business. Costing you tons in money...even costing you customers and future business. (And let's not even bring up the fines, lawsuits and audits—your personal and professional life takes a beating.)

Don't become a statistic. Take advantage of our FREE Dark Web Scan for CEOs. There's no cost... no catch... and it takes just 24 hours to get your results.

Claim your FREE Dark Web Scan today at:
<https://sysoft.ca/darkwebscan/> or call our office at (416) 410-7268.



...continued from page 3

application to load dozens of times before lunch. A sales call freezes halfway through a proposal. A team member avoids using a system altogether because it's become unreliable and frustrating.

Ask your provider:

- Are there recurring performance problems?
- Are we outgrowing our current hardware or software?
- What systems generate the most complaints internally?
- Is there anything we should optimize or replace?

Technology should support the way your team works, not train them to tolerate inconvenience. A proactive partner looks for friction before it becomes a pattern.

Question 4: Are we still compliant with industry regulations?

Compliance expectations continue to evolve, whether your business is dealing with privacy obligations, cybersecurity insurance requirements, professional standards, payment security or other industry-specific requirements.

A business that was aligned last year can drift out of alignment without realizing it if policies, controls, documentation or employee practices are not reviewed regularly.

Ask:

- Have any compliance requirements changed recently?
- Are there gaps in our documentation or policies?
- Do we need additional employee training?
- Are there security controls we should strengthen?

The cost of noncompliance extends beyond fines. It can affect insurance claims, legal exposure, operations and the confidence clients have in your business.

Question 5: What should we be budgeting for next quarter?

Good IT planning eliminates surprises.

Your provider should be tracking aging hardware, expiring warranties, software license renewals, upcoming infrastructure upgrades and security investments worth planning for.

Quarterly reviews should help you make decisions early, spread costs out intelligently and avoid emergency purchases that disrupt budgets. That is where thoughtful planning turns technology from a reactive expense into a business advantage.

Question 6: Where are we falling behind that's leaving us exposed?

This is the question that separates a

reactive provider from a true IT partner. It requires more than technical fixes. It requires strategic thinking, honest guidance and an understanding of where your business is headed.

Ask them:

- Are there new tools or automations we should consider?
- Are we lagging behind in any security protocols or performance benchmarks?
- What are other businesses our size doing that we aren't?
- Have cybersecurity standards changed in ways that affect us?

Technology moves quickly, and so do cybersecurity threats. A good IT partner helps you stay ahead by translating what is changing into clear, practical recommendations your leadership team can act on.

Silence is a red flag

If your IT provider does not have clear answers to these questions, or is not offering to meet with you quarterly, that is a warning sign.

Your business needs more than someone who reacts when something breaks. You need a partner who communicates clearly, takes accountability, responds with urgency and helps you plan thoughtfully so technology supports the business instead of slowing it down. ■