techfox REPORT

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

AUGUST 2026



THE MOST DANGEROUS RISKS IN YOUR BUSINESS

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 rarely visible right away. It’s what’s already moving underneath.

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.

During the summer, when schedules shift, employees travel and oversight gets thinner, attackers 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.

They need just one believable email. Business email compromise (BEC) works by impersonating a vendor, supplier or executive your team already trusts. The email arrives looking normal, someone pays the "vendor," and by the time anyone realizes it wasn't 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.

To ward off attackers, build a verification process for any financial request via email. A quick confirmation call to a known number stops 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. A distracted employee sees a password reset and clicks. Someone gets a text from "IT." An email arrives before a meeting requesting urgent approval.

Nobody stops to verify because stopping feels like losing time.

To fix this, 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. Speed is a weapon attackers use against you. Slowing down is how you take it away.

3. Third-party risks that travel fast

When a vendor with access to your systems is compromised, the threat travels directly into your environment. This supply chain exposure is often far greater than businesses realize.

Software tools, service providers with credentials and contractors with lingering access all present paths most owners have never mapped.

Outsourcing a service doesn't outsource accountability.

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.

techfox

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 you're talking to your IT provider only when you renew your contract, 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. That's why quarterly IT check-ins are non-negotiable if you want your business to stay protected, productive and competitive.

But here's the thing: Most business owners don't know what to ask. These are the questions your IT provider should be ready to answer every single quarter without tech-speak or vague promises.

Question 1: What security problems do we need to address?

Every business has vulnerabilities. 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 good IT provider should be able to explain where your biggest risks are today and what's being done about them.

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 don't want guesses during an outage. You want a process that's already been tested under pressure.

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

...continued on page 4

SHINY NEW GADGET OF THE MONTH

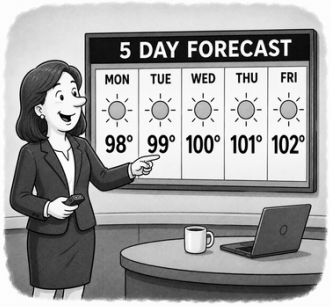
Your Laptop's New Best Friend:

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 – perfct 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"

Welcoming our New Employees



Maritza Perez
Accountnant



John Mernar
Operations Coordinator

We're excited to welcome two outstanding new team members to the TechFox family!

John Mernar, is our new Operations Coordinator. John will be supporting our projects and helping ensure everything runs smoothly across our operations.

Maritza Perez has joined our Accounting team. Maritza brings valuable years of experience and expertise to our AP and AR operations which will play an important role in supporting our financial operations.

Welcome to the team, John and Maritza—we're excited to have you both on board!

...continued from page 3

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 help your team move faster, not train them to tolerate inconvenience.

Question 4: Are we still compliant with industry regulations?

Compliance regulations change constantly, whether you're dealing with HIPAA, PCI-DSS, GDPR, cybersecurity insurance requirements or other industry-specific standards.

A company that was compliant last year can easily drift out of alignment without realizing it.

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 usually extends far beyond fines. It affects insurance claims, legal exposure and customer trust.

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 wreck budgets.

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

This is the question too many IT providers avoid because it requires strategic thinking, not just technical fixes.

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 fast, but cybercriminals move faster. A good IT partner helps you stay ahead of both.

Silence is a red flag

If your IT provider isn't meeting with you quarterly or can't answer these questions, it's time to ask why. The right partner helps you stay ahead of problems, reduce risk and make smart technology decisions.